TRABAJO ESPECIAL DE GRADO

DESARROLLO DE UNA PLATAFORMA PARA SERVICIOS BASADOS EN LOCALIZACIÓN EN LA RED GSM DE LA CORPORACIÓN DIGITEL TIM

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Maracara L., Luis L.
Para optar al Título
de Ingeniero Electricista

Caracas, 2005

TRABAJO ESPECIAL DE GRADO

DESARROLLO DE UNA PLATAFORMA PARA SERVICIOS BASADOS EN LOCALIZACIÓN EN LA RED GSM DE LA CORPORACIÓN DIGITEL TIM

Profesor Guía: Ph. D. Luis J. Fernandez
Tutor Industrial: Ing. Manuel Pérez

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. Maracara L., Luis L.
Para optar al Título
de Ingeniero Electricista

Caracas, 2005

CONSTANCIA DE APROBACIÓN

Caracas, 17 de noviembre de 2005

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Maracara L. Luis L., titulado:

"DESARROLLO DE UNA PLATAFORMA PARA SERVICIOS BASADOS EN LOCALIZACIÓN EN LA RED GSM DE LA CORPORACIÓN DIGITEL TIM"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Pilar Medrano
Prof. Pilar Medrano
Jurado

Prof. Ebert Brea
Jurado

Prof. Luis Fernández
Profesor Guía

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERIA
ESCUELA DE
INGENIERIA ELECTRICA
DEPARTAMENTO DE COMUNICACIONES

DEDICATORIA

A Dios todopoderoso quien guió mis pasos a lo largo de la carrera, quien me iluminó y entrego la sabiduría necesaria para poder alcanzar esta meta tan anhelada.

En especial a la memoria de mi padre querido Luis Maracara. Papá en donde quieras que estés siempre estarás en mi corazón. Gracias por darme lo mejor de ti para que fuese una persona exitosa, gracias por formarme el carácter y darme las directrices que hoy me llevan a alcanzar la meta, ser un INGENIERO. Se que debes estar muy orgulloso, siempre te recordaremos papá.

En especial a mi mamá quien me apoyo a lo largo de mi carrera. Gracias madre por darme la vida y el amor que necesitaba, gracias por apoyarme en las caídas y levantarme el ánimo en los momentos más difíciles.

En especial a mi hermana Marlin Maracara, quien guía, vigila y observa muy de cerca todos los pasos que doy. Gracias por haberme brindado tu cariño y apoyo incondicional, gracias por ser mi segunda mamá. Gracias hermana por entregarme tu amor como se le entrega a un hijo. Se lo mucho que te has esmerado por darme lo mejor, de verdad que el amor que me has dado no tiene límites. Lograste el objetivo que mi padre un día se propuso, llevarme hasta la universidad y que lograse un título, el título de "INGENIERO". Se lo orgullosa que te sientes de mí, te quiero mucho.

En especial a mi tía la Dra. Doris Ledezma, tía de verdad que la quiero en exceso. Gracias por su apoyo y aporte para lograr esta meta. Usted es ejemplo de constancia y dedicación, ha logrado cosas que solos los inmortales logran. Definitivamente tía como decimos en nuestro argot "Emburramos". A otra cosa tía hermosa, usted es mi tercera mamá.

A mis hermanos Luís A. Maracara L. y Valentin Ledezma. Viste hermano que ingeniería es fácil, solo es cuestión de esfuerzo y dedicación. Gracias por brindarme su apoyo, gracias por ser mis hermanos. Los quiero mucho muchachos.

A mis sobrinos, a Eduardo Soto e Ildegar Quintana. Gracias por ser tan especiales conmigo. Los quiero mucho, sin su apoyo no podría haber logrado esta meta.

A mi abuelo y abuela, a mis tías y primos. Gracias por siempre haberme dado un puesto especial en la familia.

RECONOCIMIENTOS Y AGRADECIMIENTOS

En el camino hasta la meta conocí personas tan especiales y valiosas que sería difícil olvidarlas y no mencionarlas en estos agradecimientos.

A mi pana del alma ***Austin M. Martinez Q.****, aquí lo resalto en negritas como para que no quede dudas de que usted forma parte de este logro. Sin tu apoyo habría sido más difícil alcanzar la meta. Aquí lo espero, del lado de los ingenieros eléctricos, tranquilo que ya te tocará.*

Como pasar por alto a otro de mis altos panas, el ***Ricardo J. Rodríguez D****. Gracias por el apoyo y la solidaridad brindada, amigos como tú pocos. Ah, también te resalte en negritas para que no te piques con el Austin.*

A mis amigos especiales ***José Barillas*** *y* ***Mayra Mijares****. Gracias José por permitirme ser parte de tu entorno. Mayrita Bella, no te nombre el día de la presentación de la tesis, pero aquí eres impelable. Los quiero mucho.*

A mis amigos de la universidad: Arlis Díaz (Bun Bun), Ivan Zerpa, Dubravka Romero, Gustavo Expósito, Juan F. García, Alberto (Girl), Paula de Curtis.

A la familia Quintana Fuentes, Salazar Navarro, Urbaneja Jiménez. Gracias por el cariño.

A todos mis amigos de la Corporación Digitel Tim. Gracias por el apoyo y el cariño brindado.

Al señor ***Manuel Pérez Gerente de Red de Acceso en la Corporación Digitel TIM****, a* ***George Cardozo Coordinador de Telefonía Básica y Pública****, a* ***Cesar Cabarela Coordinador de planning RF****.*

A dos personas especiales de la Coordinación del Telefonía Básica y Pública de la Corporación Digitel TIM: A lo más bello de la coordinación, ***Gudreski Díaz*** *y al gran pana* ***Juan De Abreu****. Gracias por el apoyo, el cariño y el aprecio que me han brindado. Se les quiere muchachos.*

A Nubia, una persona tan especial que sería difícil olvidar. Te quiero mucho.

A todas aquellas personas que de una u otra manera forman parte de este logro.

Gracias a la vida...

Maracara L., Luis L.

DESARROLLO DE UNA PLATAFORMA PARA SERVICIOS BASADOS EN LOCALIZACIÓN EN LA RED GSM DE LA CORPORACIÓN DIGITEL TIM

Prof. Guía: Ph. D. Luis J. Fernandez. Tutor Industrial: Ing. Manuel Pérez.

Trabajo Especial de Grado. Caracas, U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Año 2005, 109 p.

Palabras Claves: GSM (*Global System for Mobile Communications*), SIM (*Subscriber Identity Module*), SMS (*Short Message Service*), LBS (*Location Based Services*).

Resumen. En la actualidad existen diversos métodos que son capaces de estimar la ubicación de un móvil con cierta precisión, desde técnicas basadas en la celda que da cobertura al móvil, técnicas basadas en la red, técnicas basadas en la modificación del equipo y las posibles combinaciones de todas las técnicas antes mencionadas, las llamadas técnicas híbridas.

El desarrollo de la plataforma para servicios basados en localización se basa en el diseño de una aplicación que reside en la tarjeta SIM y que es capaz de enviar comandos STK al móvil para que éste devuelva los parámetros de la red que está monitoreando en ese momento. Éste despliega un menú que le permite al usuario elegir el tipo de servicio a solicitar, una vez obtenida esta información se estructura y se empaqueta para ser enviada al servidor de mensajes cortos. Cuando el servidor de mensajería recibe la información sabe a que destino enviarlo, el mismo es una aplicación del tipo ESME que monitorea permanentemente las solicitudes de localización realizadas. Una vez que esta aplicación recibe un mensaje o solicitud de ubicación, decodifica los datos y los procesa para realizar la estimación de la ubicación del usuario. Para esto se diseñó un método que se apoya en la información de la huella de cobertura de la red llamado “Drive Test”; con esta información y la arrojada por el teléfono se desarrolló un método que es capaz de estimar la posición de un móvil con una precisión de aproximadamente 148 metros de error promedio; valor bastante aceptable al compararlo con otros métodos existentes hoy en día.

Una vez que la aplicación encuentra la posición del usuario, consulta una base de datos que contiene la información de los posibles servicios demandados; para luego devolver en uno o varios SMS la información solicitada.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ACRÓNIMOS

AuC: Authentication Centre
BCCH: Broadcast Control CHannel
BSC: Base Station Controller
BSIC: Base transceiver Station Identity Code
BSIC: NCELL BSIC of an adjacent cell
BSS: Base Station Subsystem
BTS: Base Transceiver Station
CDMA: Code Division Multiple Access
CI: Cell Identity
DTX: Discontinuous transmission
ECI: Enhanced Cell Identity
EEPROM: Electrical Erasable Programable Read Only Memory
EIR: Equipment Identity Register
ETS: European Telecommunication Standard
ETSI: European Telecommunications Standards Institute
GMSC: Gateway Mobile-services Switching Centre
GMSK: Gaussian Minimum Shift Keying (modulation)
GSM: Global System for Mobile communications
HLR: Home Location Register
IMEI: International Mobile station Equipment Identity
IMSI: International Mobile Subscriber Identity
ISDN: Integrated Services Digital Network
ISO: Internacional Standard Organization
LA: Location Area
LAC: Location Area Code
MAR: Message Application Router
ME: Mobile Equipment
MCC: Mobile Country Code
MS: Mobile Station
MSC: Mobile Services Switching Center
MSISDN: Mobile Station International ISDN Number
NMR: Network Measurement Results
NMC: Network Management Center
NSS: Network Switching Subsystem
OMC: Operation Maintenance Center
PSTN: Public Service Telephone Network
PDU: Protocol Data Unit
RAM: Random Access Memory
RXLEV: Received signal level
RXQUAL: Received Signal Quality
ROM: Read Only Memory
SIM: Subscriber Identity Module
SME: Short Message Entity
SMS: Short Message Service
SMSC: Short Message Service Centre

SS7: Signalling System No. 7
STK: SIM Toolkit
TA: Timing Advance
TDMA: Time Division Multiple Access
TMSI: Temporary Mobile Subscriber Identity
UMTS: Universal Mobile Telecommunications System
VLR: Visitor Location Register

CAPÍTULO I

INTRODUCCIÓN

1.1. Planteamiento del problema

Han sido muchos los factores que han impulsado el desarrollo de los sistemas de localización en redes celulares. Uno de los países que mostró gran interés en desarrollar este sistema fue el de los Estados Unidos. Todo comenzó por el interés que presentó la FCC (Comisión Federal de Telecomunicaciones) a través de un mandato legislativo el cual le fue difundido a los operadoras de telefonía celular en el año 1996, éste planteaba que toda operadora debía ser capaz de ubicar a cualquier usuario que realizara una llamada de emergencia.

Otra de las causas que ha impulsado el desarrollo de esta tecnología es el mercado que se puede desenvolver en torno a ella. Se pueden desarrollar una variedad de servicios de gran demanda basados en la posición del móvil. Cuando se habla de localización o posición de un dispositivo móvil, esto consiste en determinar la posición de dicho terminal, con cierto grado de precisión en la red. Esto no es más que poder estimar la ubicación del usuario en función de parámetros de la red reportados al móvil. Para ello se han desarrollado diversas técnicas y métodos que se pueden emplear, todo depende del grado de exactitud que se desee y del impacto económico que se pueda tolerar, tanto a nivel de usuario, como a nivel de la operadora de telecomunicaciones.

Estas nuevas tecnologías de posicionamiento basadas en el móvil han llamado la atención de muchos proveedores de servicios de telecomunicaciones, ya que pueden desencadenar una gama de productos y servicios que se pueden ofrecer al usuario como servicios de valor agregado. Algunos servicios son:

(a) Servicios por activación automática, es decir; servicios que se inician cuando el usuario entra en una zona que ha sido predeterminada para ofrecer cierto tipo de servicio. Son idóneos para el desarrollo de aplicaciones del tipo publicitarias o de cobro, dicho de otra manera aplicaciones de facturación.

(b) Servicios que sean capaces de ofrecer información basado en la posición del usuario. Con este servicio se le puede indicar al usuario la información de distintos tipos de establecimientos cercanos (restaurantes, hoteles, farmacias, centros comerciales, etc.) a su posición.

(c) Servicios de seguimiento. Este tipo de servicio permite saber la posición de vehículos y personas tanto a nivel corporativo como para uso personal. En este caso la información de la posición puede ser requerida por un tercero autorizado para conocer la posición en todo momento.

(d) Servicios de asistencia al usuario final. Servicios de asistencia en carretera u otros servicios de emergencia están dentro de este grupo.

Las operadoras de telefonía móvil siempre han introducido servicios de gran demanda con el fin de diferenciarse de sus competidores. Las tecnologías para ofrecer servicios basados en localización son actualmente unas de las más innovadoras y lucrativas, es por ello que tantas empresas de telecomunicaciones tienen puestos sus ojos en ellas como la alternativa para brindar y desarrollar los más ambiciosos servicios de valor agregado a su red, en una era donde la innovación es la clave del éxito para mantenerse en pie y estar a la vanguardia en cuanto a tecnología se refiere.

1.2. Objetivos del proyecto

1.2.1. Objetivo general

Desarrollar una plataforma de localización en la red GSM que permita ofrecer servicios básicos en función a la ubicación que presenta el usuario en ese momento. La cantidad de servicios que se puedan brindar dependerá de la precisión al momento de realizar la ubicación.

1.2.2. Objetivos específicos

(a) Desarrollar e implementar un programa residente en la SIM Card, que contendrá el menú de aplicaciones y extraerá los parámetros de la red necesarios para realizar la ubicación del usuario.
(b) Desarrollar e implementar el programa en el servidor de aplicaciones que permita recibir y descifrar los datos enviados desde un equipo móvil a través de un SMS.
(c) Proponer e implementar los métodos para la determinación de la ubicación geográfica del móvil.
(d) Proponer e implementar los métodos para la selección de los servicios más cercanos al usuario.
(e) Validar los métodos propuestos mediante pruebas del sistema de localización en la ciudad de Caracas.

1.3. Justificación del proyecto

La corporación Digitel Tim desea implementar una plataforma que le permita realzar el potencial que posee la tecnología GSM desarrollando servicios de alta demanda que sean rentables y sostenibles en el tiempo.

Este es el caso de las aplicaciones basadas en la posición del terminal móvil. Son muchos los servicios que se pueden brindar a los usuarios finales con este tipo de aplicaciones, que no solo realza el poder de GSM, esto la pone a la vanguardia de las empresas de telecomunicaciones y la hace cada vez más competitiva en un mundo donde la innovación es la clave del éxito.

Digitel Tim ve un gran mercado en este tipo de aplicaciones que se han implementado y vienen implementando con éxito en los países del continente Europeo y actualmente en Latinoamérica, ya que ofrecen diferentes tipos de aplicaciones que van desde la ubicación de servicios básicos (restaurantes, hoteles, tiendas, estaciones de gasolinas, farmacias, etc.), localización de usuarios en un mapa, hasta el monitoreo de vehículos y flota de camiones, entre otros.

1.4. Alcance del proyecto

El presente desarrollo no abarca la implementación de la plataforma de localización en su totalidad en la red GSM de Digitel Tim. El desarrollo principal se hace para la zona de Caracas, en donde se realizan las pruebas de la fase inicial del sistema. Esta se puede extender una vez desarrollada la plataforma original y verificada su funcionalidad, a toda la red de Digitel. La cantidad de tiempo empleada en el proyecto se estimó en cuatro meses para el desarrollo y dos meses de pruebas para verificar el comportamiento y eficiencia del sistema.

1.5. Limitaciones de la investigación

Una de las principales limitaciones en esta investigación es el uso de los datos del drive test, estos son usados por los administradores de la red celular con la finalidad de verificar el comportamiento de la infraestructura de telecomunicaciones instalada. Esta herramienta les permite verificar el comportamiento real de la red. Generalmente es usada para verificar el nivel de

potencia recibida en ciertas localidades, análisis de interferencias y ver la huella de cobertura del sistema GSM. Una vez procesada esta información, los encargados de estudiar el comportamiento de la red, la despliegan en mapas donde es más fácil su estudio y visualización. Esta información es usada como parte fundamental de la plataforma desarrollada en esta investigación y como es una información muy variante y depende de muchos factores como el cambio constante, configuración e instalación de nuevas estaciones a la red; esto ocasiona que cambien los datos previamente registrados y se convierta en una limitante importante a la hora de desarrollar el servicio.

Otra de las limitaciones encontradas es que algunas de las aplicaciones desarrolladas en la tarjeta SIM no son soportadas por todos los teléfonos. Para desarrollar los programas en las tarjetas SIM se utilizan comandos especiales de una aplicación llamada SIM Application Toolkit, la cual provee los mecanismos que le permiten a las aplicaciones existentes en la SIM interactuar y operar con el equipo móvil el cual soporte los mecanismos específicos requeridos por dichas aplicaciones.

CAPÍTULO II

MARCO TEÓRICO

2.1. La tecnología GSM

2.1.1. Historia de GSM

La historia de la telefonía móvil GSM se remonta a principios de la década de los ’80, en la cual los sistemas telefónicos móviles analógicos ya tenían un rápido desarrollo en Europa, y por lo cual cada nación optó por desarrollar un sistema propio, generando el inconveniente de incompatibilidad con los sistemas desarrollados en otros países. Tal situación creó un clima no agradable debido a la no operabilidad entre los sistemas, porque no sólo debían limitar su operatividad dentro de los confines nacionales, sino que también creaba un mercado muy limitado para los varios tipos de preparaciones necesarias a la implantación y al desarrollo de las redes, por tales motivos no era viable realizar mercados de gran escala con los consiguientes ahorros tanto a favor del usuario como de los operadores de red.

Para el año 1982, un proveedor de servicios de telefonía móvil en los países nórdicos (Nordic PTT) presentó una propuesta al *Conference Européenne de Postal et Tèlécommunications* (CEPT –Conferencia Europea de Postales y Telecomunicaciones-) con la finalidad de implementar un servicio de telefonía móvil europeo que fuese común para los países pertenecientes a la comunidad y el cual operara en la frecuencia de los 900 MHz. Con la propuesta el CEPT decidió formar el *Groupe Speciale Mobile* (del cual provienen las siglas GSM) a fin de desarrollar un estándar de comunicaciones móviles para la comunidad europea. Actualmente el acrónimo GSM se utiliza para *Global System for Mobile Communication* (Sistema Global de Comunicaciones Móviles).

En el año 1985 el Grupo decidió implementar los servicios basándose en los sistemas digitales, y para el año 1987 se optó por la solución de banda estrecha

(*Narrowband*) por sobre la solución de banda ancha (*Broadband*). Finalmente en mayo de 1987 se eligió la solución banda estrecha TDMA (*Time Division Multiple Access* -Acceso Múltiple por División de Tiempo-). Ya definido lo anteriormente expuesto, a mediados de 1987 13 naciones firmaron lo que se conoce como el Memorando de Entendimiento (MoU -*Memorandum of Understanding*-), en el cual se da por asentado que las naciones firmantes se comprometen a respetar la normativa y se comprometen a tener el mismo sistema basado en el estándar GSM operativo a partir de primeros de Julio de 1991. Conformado ya el cuerpo del estándar y unificada la normativa europea en el sector de las telecomunicaciones comenzaron a ofrecer los primeros servicios comerciales de la tecnología a mediados de 1991. Ya en 1993 estaban operando 36 redes GSM en 22 países. Se agregaron normativas a las ya planteadas con la finalidad de incluir una interfaz aérea en la banda de los 1800-1900 MHz. Particularmente a los Estados Unidos de América se le ha concedido la banda de los 1900 MHz y a Europa y a los otros países extranjeros la de los 1800 MHz.

En el estándar GSM se congregan una serie de mejoras e innovaciones con respecto a los sistemas de redes celulares existentes, entre los que se puede mencionar:

(a) Uso eficiente del espectro RF (Radio frecuencias).

(b) Seguridad de la transmisión de la información, introduciendo mejoras en la calidad de las conversaciones.

(c) Reducción en los costos de los terminales de los usuarios, en infraestructura, gestión y mantenimiento de la red.

(d) Una mayor capacidad para soportar nuevos servicios y con una plena compatibilidad con la red ISDN (*Integrated Services Digital Network -Red Digital de Servicios Integrados*-) y con otras redes de transmisión de datos.

Otras de las características que hacen de GSM una red única, es que es el primer sistema estandarizado que utiliza técnicas de transmisión digital sobre el canal de radio. Otra característica importante del sistema es el *roaming* (movilidad

dentro de redes GSM). El roaming es completamente automático dentro de todas las redes del sistema GSM. Además de ofrecer la posibilidad de efectuar roaming, el estándar GSM brinda una mayor cantidad de servicios en voz y datos.

Las redes desarrolladas en la tecnología GSM ofrecen y disponen de un gran número de “Interface Open” capaces de ofrecer la interoperatividad entre equipos de diferentes proveedores, garantizando así el servicio y mantenimiento de los sistemas debido a que son equipos estándar y no del tipo propietario.

En resumidas cuentas el sistema GSM posee características especiales y que no son cubiertas por otros sistemas de telefonía celular. El comité que desarrolló este estándar en su momento buscaba una serie de objetivos, entre ellos se encontraba el que fuese posible el uso del mismo equipo en los países que integran la comunidad europea y en países no pertenecientes a ella pero que utilizan tecnología GSM, esto no es más que la posibilidad de realizar *roaming*. Otros de los objetivos era garantizar la confidencialidad de las conversaciones, es decir; seguridad en la transmisión. Buscaban calidad en el canal de voz para lo cual desarrollaron una técnica de transmisión digital que fuese compatible con los estándares internacionales.

2.1.2. Introducción técnica a GSM

La característica principal de un sistema celular reside en los enlaces y conexiones existente en éste: enlaces entre los equipos terminales de radio, enlace entre las estaciones radio bases (nodos de la red) y los equipos móviles, conexión con la base de datos donde se almacena la información y registro de cada usuario, conexión de la red celular con las redes de telefonía (Red PSTN) y las redes de datos. Todas ellas con el fin de identificar los terminales móviles, a fin de estabilizar, controlar, terminar las conexiones y actualizar los datos de gestión y así ofrecer una mejor calidad de servicio.

Un factor importante en los sistemas móviles celulares para el desarrollo de la red es el espectro de frecuencia disponible, de hecho el número de frecuencias de radio asignado a estos servicios es limitado. Éste factor es una limitante al momento de ofrecer servicios que demanden mayor ancho de banda.

Con la finalidad de optimizar y garantizar al máximo el ancho de banda disponible, a fin de servir a una mayor cantidad de usuarios en el mismo instante y en la misma zona, la red se estructura subdividiendo la zona de operación en subzonas llamadas celdas. Cada celda tiene una Estación Radio Base que opera sobre un conjunto de canales de radio, diferentes a los utilizados en las celdas adyacentes, para evitar interferencias. Este tipo de subdivisión permite la reutilización de las mismas frecuencias en celdas no adyacentes. La unión de las celdas, que en su conjunto utilizan todo el espectro de radio disponible, se llama cluster. Generalmente se utilizan formas regulares de celdas y por tanto de clusters para cubrir un área de servicio. Teóricamente las celdas se pueden imaginar con forma hexagonal, aunque en realidad son de forma irregular a causa de la no homogénea en la propagación de la señal de radio, debido principalmente a la presencia de obstáculos (edificios, árboles, etc) y a las anomalías del terreno. Reduciendo el diámetro de las celdas es posible aumentar la capacidad del sistema, aunque el uso de esta elección supone la disminución de la distancia de reutilización de las frecuencias, es decir de la distancia entre dos celdas co-canal, que conlleva el aumento de la interferencia conocida como interferencia co-canal.

De acuerdo a García, el estándar GSM utiliza la tecnología de acceso por división de frecuencia (FDMA) combinada con la de acceso por división de tiempo (TDMA), 8 canales vocales Full rate o bien 16 en Half rate multiplexados en un único canal de radio, junto a las informaciones de control de error, necesarias para disminuir la interferencia debida al ruido, y a las informaciones de sincronización y señalización. [1]

Esta es una de las primeras tecnologías que incluyen la técnica de transmisión digital sobre el canal de radio.

2.1.3. Arquitectura básica de la red GSM

El sistema GSM está compuesto por cuatro subsistemas fundamentales que cumplen funciones específicas y únicas dentro de la red. Estos se encuentran interconectados por medio de interfaces del tipo abiertas. Entre los principales subsistemas y elementos que la integran se tiene:

(a) MS (*Mobile Station*)

- ME (*Mobile Equipment*)
- SIM (*Subscriber Identity Module*)

(b) BSS (*Base Station Subsystem*)

- BSC (*Base Station Controller*)
- BTS (*Base Transceiver Station*)

(c) NSS (*Network Switching Subsystem*)

- MSC (*Mobile Services Switching Center*)
- HLR (*Home Location Register*)
- VLR (*Visitor Location Register*)
- AUC (*Authentication Center*)
- EIR (*Equipment Identity Register*)

(d) NMC (*Network Management Center*) ó NMS (*Network Management Subsystem*)

- OMC (*Operation and Maintenance Center*)

En la siguiente figura se muestra la arquitectura básica de la red GSM.

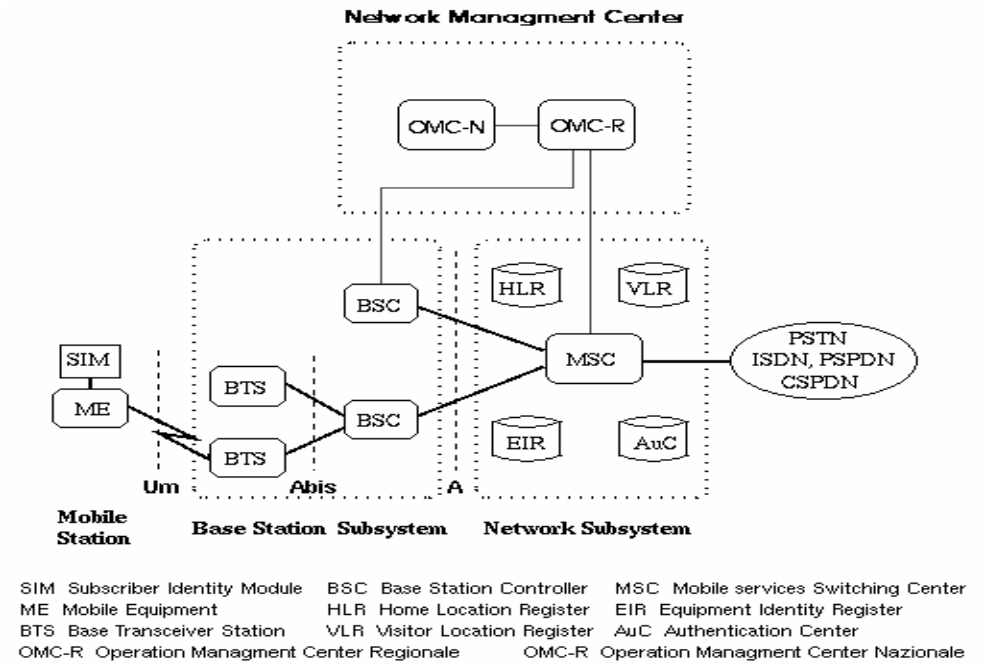

Figura 2.1. Arquitectura básica de la red GSM [1]

En la figura 2.1 se muestra cómo se interconectan todos los subsistemas que componen una red GSM, aunque más adelante se describirán con detalle sus características y funcionalidades.

2.1.3.1. Mobile Station

La MS (*Mobile Station*) es la unión de dos elementos de la red GSM, uno es la tarjeta SIM (*Subscriber Identity Module*), la cual es una pequeña tarjeta electrónica que posee memoria y un microprocesador; y es la encargada de contener toda la información referente al usuario. El otro elemento es el ME (*Mobile Equipment*), es decir; el equipo móvil propiamente dicho.

[1] Fuente: http://www.info-ab.uclm.es/labelec/Solar/Comunicacion/Telefonia_movil/index_archivos/Page1167.htm.

2.1.3.1.1. Mobile Equipment

Este se diferencia de manera única en cualquier red GSM a través del IMEI (*International Mobile Equipment Identity*). El IMEI es el único serial que puede identificar a un móvil en cualquier red GSM a nivel mundial y es utilizado para validar la autorización de acceso de equipos móviles a redes GSM.

De acuerdo a la potencia que transmiten sobre el canal de radio los equipos GSM pueden clasificarse en cinco clases. Dependiendo de la potencia emitida, estos tendrán la capacidad de alejarse de la BTS (*Base Transceiver Station*) sin perder la comunicación.

En la siguiente tabla se observa esta clasificación.

Tabla 2.1. Clases de potencia para el MS. [2]

CLASE	POTENCIA MÁXIMA (Watt)	TIPO
1	20	Vehicular
2	8	Portátil
3	5	Celular
4	2	Celular
5	0.8	Celular

Una de las características y aspectos más importantes de la MS es la capacidad que ésta posee para variar la potencia de transmisión de manera dinámica en 18 niveles diferentes, de manera que mantiene el valor apropiado y óptimo con la finalidad de evitar y limitar las interferencias co-canal que son introducidas por estaciones cercanas. Otro aspecto importante es que de esta manera se reducen los consumos de energía en el equipo y hace que el tiempo de autonomía de la batería del equipo sea mucho mayor. Este se mejora aun más con el sistema DTX (*Discontinuous Transmission*), el cual hace que no se transmita sobre el canal de radio cuando no se habla gracias a la función VAD (*Voice Activity Detection*) que se encarga de detectar la presencia de actividad vocal.

[2] Fuente: http://www.info-ab.uclm.es/labelec/Solar/Comunicacion/Telefonia_movil/index_archivos/Page1167.htm.

2.1.3.1.2. SIM

La tarjeta SIM es la encargada de resguardar los datos e identificación del suscriptor. A ella se le confía la seguridad y confidencialidad de los datos. Esta posee el IMSI (*International Mobile Subscriber Identity*), el cual es usado para identificar al usuario de manera única en cualquier red GSM. La tarjeta SIM posee además algoritmos que son usados para encriptar la señal de radio, para que de esta manera se pueda garantizar la confidencialidad de las comunicaciones. De la misma manera ésta posee en su interior una contraseña de restricción que permite el acceso a los datos internos de ésta y evita accesos no autorizados a la información contenida en su interior. También posee una memoria capaz de almacenar números telefónicos, mensajes de texto y cualquier otro tipo de información en su interior.

2.1.3.2. Base Station Subsystem

El BSS (*Base Station Subsystem*) es el encargado del control de todo lo correspondiente a la interfaz de radio. La interfaz de radio o el BSS, se compone de un conjunto de BTS (*Base Transceiver Station*) asociadas a una BSC (*Base Station Controller*), la cual es la encargada de controlar al conjunto de BTS. Los elementos del BSS se comunican a través de una interfaz estandarizada del tipo Abis, esto con la finalidad de permitir interoperatividad con componentes y equipos de distintos fabricantes. Aparte de la interfaz Abis existe otra interfaz que se usa para comunicar a la BSC con el MSC (*Mobile Switching Center*), esta es la interfaz tipo A.

2.1.3.2.1. Base Transceiver Station

Esta contiene las unidades encargadas de transmitir y recibir las señales de radio, es decir; contiene los transmisores y receptores que prestan y ofrecen servicio en una celda, proporcionando de esta manera una interfaz entre los equipos móviles y las BSC.

Estas llevan a cabo una serie de funciones que se describirán a continuación:

(a) Capacidad de configurar canales en *Full Rate* y *Half Rate*.
(b) Permiten el uso de diversidad en espacio para contribuir a la mejora de la señal en la recepción. Dicho de otra manera, la colocación de dos antenas en el equipo de recepción con la finalidad de ayudar a mejorar la calidad de la señal recibida.
(c) Poseen la capacidad de monitorear el ROE, es decir; la relación de ondas estacionarias en la antena.
(d) Se le puede configurar el *Frequency Hopping*. Esto con la finalidad de mejorar la calidad de la señal en el canal de radio con el cambio de la frecuencia.
(e) Se puede habilitar el DTX (*Discontinuous Transmission*), bien sea en el canal de subida (*up-link*), así como en el canal de bajada (*down-link*).
(f) Gestiona los algoritmos de encriptamiento para la transmisión sobre el canal de radio, garantizando así la confidencialidad de la información transmitida por el usuario.
(g) Realiza el monitoreo del enlace de radio realizando mediciones de las señales recibidas, que posteriormente le serán enviadas a la BSC para garantizar la calidad de la señal sobre el canal de radio.

2.1.3.2.2. Base Station Controller

La BSC (*Base Station Controller*) administra y gestiona los recursos de radio de un conjunto de BTS, manteniendo de esta manera el control en todo momento de las conexiones entre la BTS y el MSC. Aparte de esto es la encargada de gestionar los canales de radio, los niveles de potencia de las señales, el proceso del *frequency hopping* y los procesos de *handover*.

En general su labor es:

(a) La administración y configuración de los canales de radio para que en el establecimiento de una llamada se elija la celda adecuada y los canales de radio óptimos para el establecimiento de la conexión.

(b) Gestiona y decide los procesos de *handover* en base a las medidas que se efectúan sobre los canales de radio y que le son enviadas por las BTS. El *handover* es el proceso que permite al móvil cambiar de celda cuando este lo requiere, ya sea porque se encuentra en los límites de una celda o por escasos niveles de recepción del lado del receptor; esto a fin de garantizar la comunicación en todo momento.
(c) Realiza las funciones de transcodificación de los canales de radio en *Full Rate* (16 kbps) o *Half rate* (8 kbps) sobre canales de 64 Kbps.

2.1.3.3. Network Switching Subsystem

Este subsistema de conmutación de red es el encargado de realizar las funciones de enrutamiento de las llamadas de los usuarios móviles con otros usuarios y con los usuarios de la red de telefonía fija a través del MSC. Este también hace la función de base de datos a través de cuatro elementos de red como el HLR, VLR, AUC y el EIR. Esto para la identificación, la autenticación de los equipos y usuarios en la red.

2.1.3.3.1. Mobile Switching Center

Este es uno de los componentes principales y centrales del NSS y de la red GSM. El mismo se encarga, basado en información que le llega desde dispositivos como el HLR y el VLR, del manejo y administración de todas las llamadas que se generan en la red y las provenientes de otras redes. Además éste cumple las funciones de *gateway* con otros componentes del sistema, gestionando los procesos de *handover* de las llamadas en curso entre BSC distintas o enrutándolas hacia otros MSC. En una red puede existir más de un MSC, de modo que cada uno se ocupará y atenderá a un conjunto de BSS.

Algunas de las funciones fundamentales del MSC son:

(a) Proceso de autenticación de la llamada. Esto es un proceso fundamental debido a que en él se determina si el usuario está autorizado para realizar llamadas y de qué tipos de servicios puede disfrutar.

(b) Mantiene la confidencialidad de la identidad del usuario. “Para garantizar la confidencialidad acerca de la identidad del usuario en el canal de radio, aún estando ya todas las informaciones criptografiadas, el sistema no transmite nunca el IMSI asignado, sin embargo se le asigna el *Temporary Mobile Subscriber Identity* (TMSI), que se asigna en el momento de la llamada y tiene un significado temporal. Crear la correspondencia entre TMSI e IMSI es tarea del MSC y cuando el móvil se desplaza a una *Location Area* controlada por otro MSC, se le tiene que asignar un nuevo TMSI.” [1] De esta manera se evita que se transmita información confidencial del suscriptor y que pudiese ser usada para realizar fraudes en la red.

(c) Administra los procesos de *handover*

2.1.3.3.2. Home Location Register

Toda la información de los usuarios de la red GSM para su identificación dentro del sistema se guarda en el HLR. É ste tiene la función de comunicarle al VLR algunos datos correspondientes al usuario en el momento que éstos cambien de una *Location Area* a otra. El HLR en su interior identifica a los usuarios a través del MSISDN (*Mobile Station International ISDN Number*), el cual es el número que se le asigna al suscriptor y lo identifica de manera única en la red telefónica internacional.

El HLR es básicamente una base de datos que guarda información, el mismo puede ser único en la red o puede ser del tipo distribuido. De esta manera se pueden tener MSC sin HRL pero éstos se deben conectar al HLR de otros MSC. En el caso de que exista más de un HLR a éstos se le debe asignar un área de numeración.

El HLR contiene en su interior una serie de datos que son usados en el momento que se genera la llamada. Estos son el IMSI (*International Mobile Subscriber Identity*), el MSISDN y los tipos de servicio de los cuales puede disfrutar el usuario como voz, datos, envío de SMS, llamadas internacionales entre otros. Aparte de esto contiene la información de la posición del móvil en todo momento conociendo en qué VLR se encuentra registrado.

En resumen las funciones que realiza el HLR son:

(a) Seguridad. Se comunica con el AUC y el VLR con la finalidad de realizar la autenticación del usuario.
(b) Conocimiento de la posición del móvil. Interactúa con el VLR para conocer bajo qué celda se encuentra registrado.
(c) Asigna el precio de la llamada. Comunicación con el MSC
(d) Administración de los datos del suscriptor. En su interior posee todos los datos de los usuarios de la red, que además le suministra al OMC y el VLR.
(e) Manejo de las estadísticas de las llamadas. Los datos almacenados le son enviados al OMC para su futuro procesamiento.

2.1.3.3.3. Visitor Location Register

El VLR es la base de datos que se encarga de almacenar de manera temporal todos los datos relacionados a los suscriptores que se encuentran bajo su control. Los datos del usuario les son solicitados al HLR donde pertenece. Una manera de simplificar la implementación de los sistemas en la red, es la de integrar el VLR junto al MSC, de manera que el área controlada por el MSC sea la misma para el VLR.

Dentro de las informaciones que contienen se tiene el TMSI que se usa para garantizar la confidencialidad y seguridad del IMSI, el estatus del móvil; es decir, si se encuentra apagado en *standby* u ocupado. Contiene información de los servicios suplementarios activos como por ejemplo llamada en espera, llamadas

en conferencia entre otros, además de los tipos de servicio de los cuales puede disfrutar el usuario.

2.1.3.3.4. Autentication Center

El centro de autenticación AUC, es el encargado de verificar si los servicios demandados han sido solicitados por un suscriptor autorizado y legítimo, y no por terceros. Básicamente el sistema de autenticación consiste en verificar si la SIM es legítima antes de enviar la información del abonado sobre el canal de radio; es decir, no se transmite información del suscriptor sin antes saber si la solicitud de acceso corresponde a un usuario legítimo y no a una tarjeta clonada. Para esto se generan códigos y claves de manera aleatoria mediante algoritmos definidos en el estándar y que son grabados tanto en la tarjeta SIM como en el AUC.

La autenticación se realiza cada vez que un usuario desea conectarse a la red y en los siguientes casos:

(a) Siempre que el móvil genere y reciba una llamada.
(b) En los momentos que se actualiza la posición del móvil, es decir; en los procesos de *location update.*
(c) Siempre que el usuario haga uso de los servicios suplementarios como llamadas en espera, llamada en conferencia, entre otros.

El AUC se implementa junto al HLR el cual es el único sistema con el cual se encuentra interconectado y es el único con el cual se comunica.

2.1.3.3.5. Equipment Identity Register

El EIR (*Equipment Identity Register*) es la base de datos encargada de verificar si el móvil está autorizado para acceder a la red, mediante la comprobación del IMEI. Esta se divide en tres secciones, lista blanca (*White List*), lista negra (*Black List*) y lista gris (*Grey List*). En la lista blanca se encuentran los

IMEI de todos aquellos equipos que pueden acceder a la red porque están autorizados. Además contiene los IMEI de los equipos con los que las operadoras tienen acuerdo de *roaming* internacional. La lista negra posee los IMEI de los equipos que han sido bloqueados por causas de robos u otras causas. La lista gris contiene todos los IMEI de los equipos que no han sido homologados.

En los intentos de conexión del móvil a la red, el MSC mediante el EIR verifica la existencia de al menos uno de los siguientes casos para permitirle o negarle el acceso a la red:

(a) El equipo se encuentra homologado para tener acceso a la red.
(b) El móvil no ha sido robado o utilizado de manera fraudulenta.
(c) El equipo no está marcado como faulty.

En una red GSM puede existir un solo EIR o se puede utilizar el esquema en configuración distribuida, es decir; hacer uso de más de un EIR en la red. Este se puede alojar en el mismo servidor donde se ubica el HLR y el AUC, pero por razones de seguridad se recomienda colocarlo aparte.

2.1.3.4. Network Management Center

2.1.3.4.1. Operation and Maintenance Center

El OMC (Operation and Maintenance Center) posee las siguientes funciones:

(a) Mediante el OMC se puede acceder de manera remota a todos los elementos de la red como lo son: el BSS, el MSC, el VLR, el HLR, el EIR y AUC.
(b) Se gestionan las alarmas y estatus de la red, garantizando de esta manera que la red siempre se encuentre en correcto funcionamiento y se puedan atender las fallas a tiempo.
(c) En el OMC se obtiene toda la información necesaria para el proceso de facturación.

(d) A través del OMC se visualiza la configuración actual de la red, pudiendo realizar configuraciones vía remota en cualquier momento a conveniencia de los operadores de la red.
(e) Generalmente existe un OMC por red, pero en casos donde la red es muy extensa se hace uso de más de uno, pero siendo sólo uno el principal a los restantes se le asigna el control de zonas específicas.

2.2. Las tarjetas inteligentes

En la sección anterior se hizo una introducción a la tecnología GSM. En ella se realizó una ligera descripción de la SIM (*Subscriber Identity Module*), la cual es la tarjeta donde se almacena toda la información referente al suscriptor y la que le permite acceder a la red para disfrutar de sus servicios. Esta tarjeta posee ciertas características que la hacen diferenciar de tecnologías de tarjetas inteligentes similares y es una de las partes más críticas del sistema GSM, al recaer sobre ella la responsabilidad de proteger la información del usuario y de fraudes en la red. A continuación se dará una breve descripción de los tipos de tarjetas que existen en el mercado hoy en día.

2.2.1. Tipos de tarjetas

Es muy frecuente llamar a todas las tarjetas que posean contactos dorados o plateados sobre su superficie, con el nombre de tarjetas inteligentes. Sin embargo, sobre este término es conviene hacer una clasificación más adecuada. La ISO (*Internacional Standard Organization*) prefiere usar el término “tarjeta de circuito integrado” (*Integrated Circuit Card o ICC*), para referirse a todas aquellas tarjetas que posean algún dispositivo electrónico. Este circuito contiene elementos para realizar transmisión, almacenamiento, y procesamiento de datos. La transferencia de datos puede llevarse a cabo a través de contactos, que se encuentran en la superficie de la tarjeta, o sin contactos por medios electromagnéticos.

Estas tarjetas presentan muchas ventajas en comparación con las de bandas magnéticas, algunas de ellas son:

(a) Son capaces de almacenar más información.
(b) Pueden proteger la información que almacenan en sus memorias de posibles accesos no autorizados.
(c) Poseen mayor resistencia al deterioro de la información almacenada.

Dado que el acceso a la información se realiza a través de un puerto serie y supervisado por el propio sistema operativo de la tarjeta, es posible escribir datos confidenciales que no puedan ser leídos por personas no autorizadas. En principio, las funciones de escritura, lectura y borrado de la memoria pueden ser controlados tanto por hardware como por software, o por ambos a la vez. Esto permite una gran variedad de mecanismos de seguridad, siendo el chip integrado el componente más importante.

Las tarjetas están clasificadas según el tipo de circuito como:

(a) Tarjetas de memoria.
(b) Tarjetas de memoria con circuitos de seguridad.
(c) Tarjetas con CPU o tarjetas inteligentes.
    - Tarjeta sin contactos

2.2.1.1. Tarjetas de memoria

Los datos que se requieren para las aplicaciones con tarjetas de memoria son almacenados en una EEPROM (*Electrical Erasable Programable Read Only Memory*). Los accesos a ésta no están controlados, y por tanto no existe protección contra escritura o borrado de la memoria en alguna de sus áreas.

Las funciones que desempeñan las tarjetas de memoria están optimizadas para aplicaciones particulares en las que no se requieren complejos mecanismos de seguridad. Una aplicación típica son las tarjetas de pago en cabinas de teléfono.

En la siguiente figura se muestra el esquema de este tipo de tarjeta.

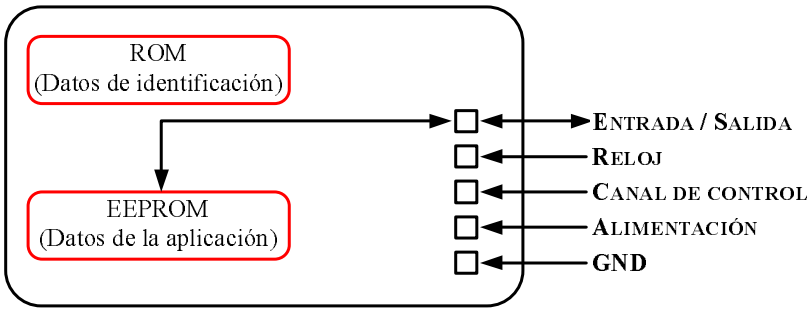

Figura 2.2. Esquema de bloques de la arquitectura de una tarjeta inteligente.

2.2.1.2. Tarjetas de memoria con circuitos de seguridad

El circuito de seguridad proporciona un sistema para controlar los accesos a la memoria frente a usuarios no autorizados. Este sistema funciona mediante el empleo de un código de acceso que puede ser de 64 bits o más. En la figura 2.3 se muestra el esquema que presenta esta tarjeta.

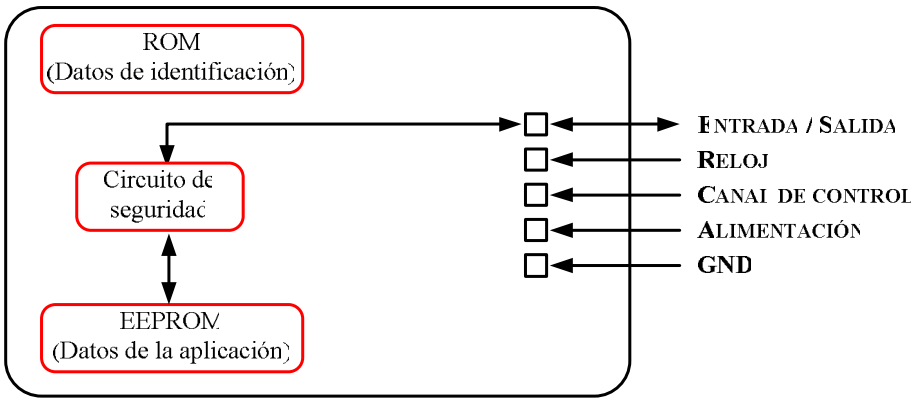

Figura 2.3. Esquema de bloques de la arquitectura de una tarjeta de memoria con circuito de seguridad.

2.2.1.3. Tarjetas inteligentes

Estas tarjetas poseen en su chip un microprocesador, que además cuenta con algunos elementos adicionales como lo son:

(a) ROM.
(b) EEPROM.
(c) RAM.
(d) Un Puerto de entrada/salida.

La ROM (*Read Only Memory*) contiene el sistema operativo de la tarjeta, y se graba durante el proceso de fabricación.

La EEPROM es la memoria no volátil del microprocesador, y en ella se encuentran datos del usuario o de aplicación, así como el código de las instrucciones que están bajo el control del sistema operativo. También puede contener información como el nombre de usuario, número de identificación personal o PIN (*Personal Identification Number*), etc.

La RAM (*Random Access Memory*) es la memoria de trabajo del microprocesador. Al ser volátil, toda la información se perderá al desconectar la alimentación.

El puerto de entrada y salida normalmente consiste en un simple registro, a través del cual la información es transferida bit a bit.

Las tarjetas con microprocesador son muy flexibles debido a que pueden realizar muchas funciones. En el caso más simple, sólo contiene datos referentes a una aplicación específica, esto hace que dicha tarjeta sólo se pueda emplear para esa aplicación, sin embargo, los sistemas operativos de las tarjetas más modernas hacen posible que se puedan integrar programas para distintas aplicaciones en una sola tarjeta. En este caso, la ROM contiene sólo el sistema operativo con las instrucciones básicas, mientras que el programa específico de cada aplicación se graba en la EEPROM después de la fabricación de la tarjeta.

En la figura 2.4 se presenta la arquitectura típica de una tarjeta con microprocesador.

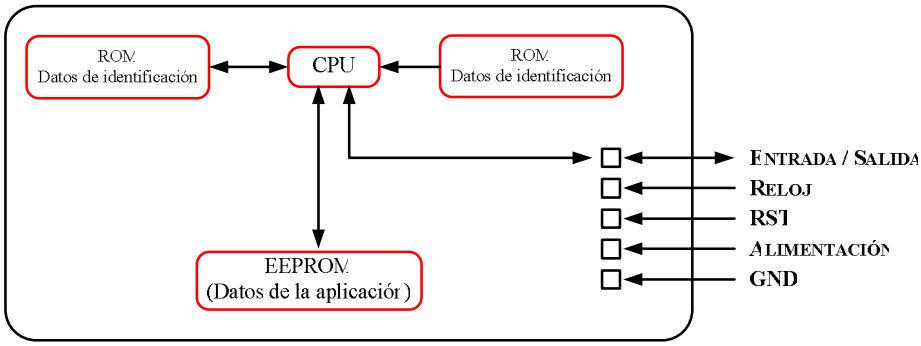

Figura 2.4. Arquitectura típica de una tarjeta con microprocesador.

2.2.1.3.1. Tipos de tarjetas inteligentes

2.2.1.3.1.1. Tarjetas sin contacto

Las tarjetas inteligentes pueden tener en su superficie unos contactos dedicados a posibilitar la comunicación de la propia tarjeta con los dispositivos exteriores. EL tamaño y la posición de estos contactos se especifican en el estándar ISO7816.

Como resultado de la experiencia conseguida en los últimos años por los fabricantes de tarjetas, la fiabilidad de estas se ha visto considerablemente aumentada, por ejemplo, la tasa de fallo en tarjetas de pago en cabinas de teléfonos es inferior al 0.001%. Sin embargo, los contactos son casi siempre los culpables de los fallos de funcionamiento. En algunos casos debido al deterioro en la superficie de contacto o debido a la suciedad adherida a los mismos.

Estos problemas técnicos son resueltos mediante el uso de tarjetas sin contactos. Además de estas ventajas, esta tecnología ofrece otras mejoras, una de ellas es la de no tener que introducir la tarjeta en un lector. Esto es una gran ventaja en sistemas de control de accesos donde se necesitan abrir una puerta u otro mecanismo, puesto que la autorización de acceso puede ser revisada sin que se tenga que sacar la tarjeta del bolsillo e introducirla en un equipo.

Este tipo de tarjetas se comunican por medio de radiofrecuencias. Según la proximidad necesaria entre tarjeta y lector, existen dos tipos:

(a) Tarjeta cercana: debe estar a unos pocos milímetros del lector para que sea posible la comunicación.
(b) Tarjeta lejana: la distancia varía entre centímetros y unos pocos metros.

Las tarjetas inteligentes fueron desarrolladas por primera vez en el Instituto Arimura en 1978. El grosor de las tarjetas puede variar entre 0.76 mm (estándar de una tarjeta de crédito) y 3 mm.

Desde el punto de vista de como se alimentan las tarjetas, tenemos dos tipos:

(a) En este primer tipo, la tarjeta posee junto al chip una batería que alimenta los circuitos.
(b) Otro tipo de tarjetas incorporan un hilo metálico incrustado. Este hilo se somete a un campo electromagnético variable que a su vez induce una corriente eléctrica capaz de alimentar los circuitos de la tarjeta.

Existe otra clasificación para las tarjetas sin contactos, según la banda de frecuencia en la que operen, éstas pueden trabajar en baja frecuencia (LF), alta frecuencia (HF) y en la frecuencia de microondas. La frecuencia de trabajo es determinada por las leyes que cada país posee para la regulación de su espacio radioeléctrico.

2.2.1.3.1.2. Tarjetas Superinteligentes

Estas cumplen las mismas funciones que las tarjetas inteligentes con microprocesador pero también están equipadas con un teclado, una pantalla LCD y una pila. Esta tarjeta puede funcionar totalmente independiente, por esto no hay necesidad de insertarla en un equipo.

Las ventajas que presenta este tipo de tarjetas son las siguientes:

(a) Gran capacidad de memoria.
(b) Altos niveles de seguridad.
(c) Reducción del fraude.
(d) Información organizada.
(e) Confiabilidad.
(f) Alto manejo de información.
(g) Seguridad en la información.
(h) Facilidad de usos sin necesidad de conexiones en línea o vía telefónica.
(i) Comodidad para el usuario.

(j) A través de Internet los usuarios de tarjetas inteligentes podrán comprar por computador y pagar por red.
(k) Garantizar operaciones económicas, 100% efectivas y a prueba de robos.
(l) Caída de los costos para empresarios y usuarios.
(m) Estándares específicos ISO 7810, 7811, 9992, 10536.
(n) Tarjetas inteligentes multiservicio.
(o) Privacidad.
(p) Administración y control de pagos más efectivo.

Las desventajas:

(a) Mayor posibilidad de virus.
(b) Molestias al recuperar información de una tarjeta robada.
(c) Por su tamaño se puede extraviar fácilmente.
(d) La tarjeta debe ser recargada.
(e) Mayor costo de fabricación.
(f) Dependencia de la energía eléctrica para su utilización.
(g) Vulnerable a los fluidos.
(h) Es necesario un lector para tarjetas inteligentes.

Las tarjetas antes mencionadas, en especial las tarjetas inteligentes, poseen características tanto físicas como eléctricas tales como dimensiones físicas, tensión de alimentación, consumo de corriente, entre otras que describen el cómo deben manipularse. También poseen protocolos especiales de comunicación debido a la existencia de un único canal de comunicaciones entre la tarjeta y los dispositivos externos, en cuyo caso ambos deben turnarse para llevar a cabo la transmisión de datos. A este procedimiento intermitente de enviar y recibir información se le denomina "*half duplex*".

El procedimiento "*full duplex*", donde cada parte puede enviar y recibir al mismo tiempo, aún no está disponible en ninguna de las tarjetas inteligentes, sin embargo, la mayoría de los microprocesadores incorporan un canal de entrada y otro de salida, y como dos contactos de los ocho disponibles de los que posee esta

tarjeta no están en uso, se podría utilizar uno de ellos para añadir una segunda vía de comunicación.

Toda comunicación que se realice con la tarjeta es iniciada siempre por el dispositivo externo, esto quiere decir que la tarjeta nunca transfiere información sin que se haya producido antes una petición externa. Esto equivale a una relación maestro-esclavo, siendo el terminal el maestro y la tarjeta el esclavo.

A continuación en la siguiente sección daremos una descripción general de la tarjeta SIM, la cual es un elemento fundamental de la red GSM.

2.3. La tarjeta SIM

La tarjeta SIM es uno de módulos de la tecnología GSM encargados de la autenticación de los usuarios en la red. Este elemento ha sido objeto de numerosos estudios que han permitido que no solo aumente su capacidad (actualmente están disponibles en el mercado tarjetas de 64Kbits y hasta de 128Kbits) sino que también sea capaz de soportar aplicaciones relacionadas a la creación de nuevos menús, almacenamiento de íconos, altos niveles de seguridad y WAP para teléfonos GSM Fase 2+.

En la siguiente sección se proporcionará una visión global de las aplicaciones soportadas por la tarjeta SIM de la red GSM.

2.3.1. Que es la tarjeta SIM

La tarjeta SIM del sistema GSM es uno de los elementos encargados de la autenticación de los usuarios en la red. Nuevas aplicaciones la han convertido, desde un módulo pasivo de almacenamiento de datos, en un micro sistema capaz

de soportar nuevos menús, comunicación de voz y SMS de forma independiente, altos niveles de seguridad, WAP, WEB y otro tipo de aplicaciones.

Figura 2.5. Tarjeta SIM. [3]

La SIM es la tarjeta insertada en el teléfono que contiene la información del usuario relacionada a su número, los servicios a los que está suscrito y la lista de redes disponibles para uso. Corresponde al grupo de las tarjetas inteligentes descritas en la sección anterior, por lo tanto están dotadas con módulos y dispositivos que no poseen las otras tarjetas; en especial poseen memoria ROM la cual posee el sistema operativo de la tarjeta, memoria EEPROM donde se almacenan los datos del suscriptor y de las aplicaciones especiales que vienen con la SIM, memoria RAM la cual es utilizada por el microprocesador de la tarjeta como memoria para realizar sus funciones y un puerto de entrada/salida para la transferencia de datos entre el móvil y la SIM.

Aparte de los módulos antes mencionados posee un elemento fundamental que marca la diferencia y es el microprocesador que viene incorporado con la tarjeta el cual es el que le permite realizar procesos especiales que no se pudieran lograr si este dispositivo no estuviese presente. Los módulos antes mencionados conforman la configuración básica de una tarjeta inteligente, aunque el creciente desarrollo en cuanto a tecnología de tarjetas se refiere puede añadirle nuevos módulos que la hagan aún más poderosas y capaces de desarrollar numerosas aplicaciones y hacerlas cada vez más robustas.

[3] Facilidades de la SIM Card por Heidi Rivas Hernández. Digitel TIM, Proyectos Especiales.

Como ya se mencionó la tarjeta SIM no actúa por sí sola, es decir; no inicia ningún proceso sin que se le haya solicitado, para que la tarjeta pueda iniciar algún proceso tiene que solicitarse e indicarle que inicie la comunicación con el móvil.

2.3.2. Aplicaciones de la tarjeta SIM

Las aplicaciones desarrolladas para la SIM les brindan a los operadores de redes GSM el despliegue de una variedad de servicios y utilidades de valor agregado el cual permite aprovechar al máximo la capacidad del sistema, desplegando servicios de gran demanda los cuales repercuten en la productividad del operador. Por eso estas aplicaciones son fundamentales a la hora de diferenciar servicios de gran demanda y marcar la pauta en cuanto a innovación tecnológica se refiere.

Entre las aplicaciones disponibles para el aumento de la gama de las utilidades disponibles para la SIM tenemos las siguientes:

(a) *SIM Toolkit* ó *SIM Application Toolkit*.
(b) *Secure Application Module* (SAM).
(c) *SIM Alliance Toolbox* (SAT).

2.3.2.1. SIM Toolkit ó SIM Application Toolkit.

SIM Application Toolkit es una extensión del estándar GSM definido por el ETSI (*European Technical Standard Institute*) entre la tarjeta y el equipo móvil que define el grupo de comandos y procedimientos necesarios para la construcción de una interfaz entre la tarjeta SIM y el móvil.

Este estándar permite:

(a) Insertar menús en la estructura de menús del equipo móvil con la finalidad de la actualización para nuevos servicios.
(b) Crear la necesidad de solicitud de información a los usuarios, por medio de los nuevos menús disponibles en su unidad móvil.

(c) Establecer llamadas o envíos SMS de forma independiente, es decir, si la nueva aplicación requiere del envío de mensajes cortos la tarjeta SIM lo hará automáticamente.

Aunque *SIM Toolkit* permite a los operadores de red desarrollar aplicaciones competitivas y de rápida implementación siempre es necesario reprogramar las tarjetas para añadir la nueva aplicación.

Por esta razón se ha logrado que, con *SIM Toolkit*, se permita esta actualización de campos de datos dentro de la SIM de forma remota. Con esta característica innovadora, el SMS se convierte en un mecanismo para la personalización de la SIM de los teléfonos GSM por medio del envío de códigos a través de mensajes cortos.

Por otro lado se tiene que *SIM Toolkit* es una aplicación aparte de la funcionalidad de comunicación GSM dentro de la SIM. Esto quiere decir que existen, dentro de la tarjeta un grupo de comandos específicos para las aplicaciones de *SIM Toolkit* y otro, totalmente independiente, para la comunicación mediante la red GSM.

Una de las dudas más comunes relacionadas con *SIM Toolkit* es aquella que se basa en la supuesta competencia entre *SIM Toolkit* y WAP.

En realidad WAP (*Wireless Application Protocol*) y *SIM Toolkit* no son vertientes competidoras sino más bien complementarias. En general, *SIM Toolkit* será usado en aquellas aplicaciones que necesitan un alto grado de seguridad, como por ejemplo banca móvil, y aquellas aplicaciones del tipo estáticas relacionadas a bases de datos como páginas amarillas y directorios de compañía. Por su parte, WAP será usado en aquellos servicios más dinámicos como Internet *browsing* (navegación web) y servicios de accesos de información variable, como las noticias.

2.3.2.2. Secure Application Module (SAM)

El SAM es una tarjeta o chip que contiene, dentro de sí, el modulo de seguridad. El SAM provee funcionalidades de seguridad que incluyen: almacenamiento de las claves de encriptación y funciones de datos y seguridad de los servicios asociados.

El módulo de aplicaciones de seguridad (SAM) es generalmente hospedado dentro de una tarjeta de circuito integrado con la finalidad de brindar una fácil instalación y fácil desinstalación en un sistema.

El módulo SAM no es característico de la tecnología GSM, de hecho no contiene información relativa a la comunicación por medio de esta tecnología, sin embargo, es un estándar que se ha usado en muchos equipos GSM sobre todo en aquellos relacionados con operaciones bancarias, por ejemplo puntos de venta móviles.

2.3.2.3. SIM Alliance Toolbox (SAT o S@T)

Es un estándar global que, con un conjunto de aplicaciones, permite el acceso a servicios WML (*Wireless Markup Languaje*) desde cualquier teléfono Fase 2+. Por medio de la plataforma asociada a S@T los operadores podrán ofrecer servicios WAP sin importar qué equipo posean sus usuarios. Vale la pena destacar que los usuarios que quieran gozar del servicio WAP con teléfonos fase 2+ deben actualizar su SIM con la aplicación en SIM Toolkit asociada al servicio de S@T.

La desventaja principal que conlleva la instalación de S@T es la adquisición de una plataforma paralela a la plataforma WAP para poder proveer este servicio a los terminales Fase 2+.

CAPÍTULO III

DESCRIPCIÓN DEL PROTOCOLO Y PROGRAMA DESARROLLADO PARA LA CONEXIÓN DEDICADA AL SMSC

3.1. El Servicio de Mensajería Corta SMS (Short Message Service)

3.1.1. Introducción al Servicio de Mensajería Corta

El servicio de mensajería corta SMS (*Short Message Service*) es un servicio que se encuentra actualmente disponible en teléfonos del tipo móvil y que permite el envío de mensajes de texto a teléfonos móviles, fijos y otros dispositivos. El *Short Message Service* fue diseñado originalmente como parte del estándar GSM. Debido a que su uso se difundió de gran manera, en la actualidad se encuentra disponible en todas las redes de telefonía celular existentes, incluyendo las redes de tercera generación.

El servicio de mensajería hace uso del SMSC (*Short Message Service Center*) el cual hace la función de servidor de mensajería para el almacenamiento y envío de mensajes. La red celular provee el medio de transporte de mensajes entre el SMSC y los equipos móviles. El SMS garantiza también la entrega de mensajes cortos a través de la red. Las fallas temporales de entrega son identificadas y el mensaje es almacenado en la red hasta que el destinatario se encuentra disponible para recibirlo.

3.2. Elementos que integran el Servicio de Mensajería Corta

En la presente sección se describirán los elementos que conforman la plataforma de mensajería corta. La interconexión de dichos elementos hace posible la interoperatividad del sistema de mensajería, debido a que cada uno cumple una función particular. Se nombrarán y describirán parte de los elementos

que conforman el sistema debido a que muchos ya fueron descritos en el capítulo anterior. A continuación se describen los elementos.

3.2.1. El Centro de Servicio de Mensajería Corta SMSC (Short Message Service Center)

El SMSC es un elemento de la red GSM que recibe mensajes de diferentes dispositivos y los mantiene almacenado en memoria mientras no logra enviarlos al destino especificado. Si el SMSC no logra enviar los mensajes inmediatamente (porque el terminal está apagado o fuera de cobertura), el tiempo máximo que serán almacenado en memoria dependerá de los administradores de la red. Transcurrido este tiempo límite los mensajes serán eliminados automáticamente del SMSC y ya no serán enviados a su destino.

Este elemento debe ser altamente confiable, debe manejar un alto tráfico de mensajes y debe tener alto rendimiento de procesamiento. Aparte debe ser fácilmente escalable con la finalidad de adecuarlo a la demanda de SMS en la red.

3.2.2. El ESME (External Short Messaging Entities)

Es el elemento que se encarga de enviar o recibir mensajes cortos. El envío o recepción de mensajes cortos puede ser hecho a través de correo de voz, web, e-mail o por otros medios destinados para tal fin.

3.2.3. El SME (Short Messaging Entities)

El *Short Messaging Entities* es un dispositivo que puede enviar o recibir mensajes. El SME puede ser localizado en redes fijas, teléfonos móviles o algún otro centro de servicio.

3.2.4. El SMS-Gateway/Interworking Mobile Switching Center

El SMS-Gateway MSC (SMS-GMSC) es un MSC capaz de recibir un mensaje corto de un SMSC, interrogando al HLR por la información de enrutamiento, y con esta información es capaz de realizar la entrega del mensaje. El SMS Interworking MSC (SMS-IWMSC) es un MSC capaz de recibir un mensaje corto de la red móvil y reenviarlo al correspondiente SMSC. El SMS-GMSC/SMS-IWMSC está típicamente integrado con el SMSC.

3.2.5. El Punto de Transferencia y Señalización STP (Signal Transfer Point)

El *Signal Transfer Point* es un elemento de red que está normalmente disponible en desarrollos de redes que permiten el estándar de interconexión para mensaje IS-41 sobre sistemas de señalización número 7 (SS7) y éste está enlazado con múltiples elementos de red GSM, tales como el HLR y el MSC.

3.2.6. Arquitectura de red básica para desarrollo del servicio de mensajería

En la siguiente figura se muestra cómo se configura la red para que el sistema sea capaz de manejar mensajes de texto.

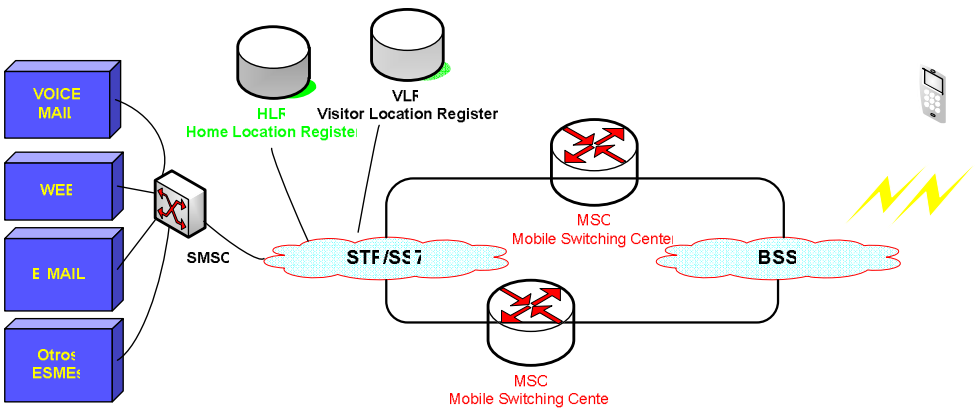

Figura 3.1. Arquitectura básica del sistema de mensajería corta de texto

3.3. Protocolo utilizado para la comunicación entre el SMSC y ESME

3.3.1. El protocolo SMPP (Short Message Peer to Peer)

El protocolo SMPP, es un protocolo abierto el cual proporciona una interfaz de comunicación flexible, diseñada para la transferencia de mensajes de texto entre aplicaciones externas y los SMSC de las diferentes empresas de telefonía celular. Fue creado por la compañía Logica CMG, fue publicado y adoptado como estándar; éste es controlado por el SMS Forum, el cual era anteriormente llamado SMPP Forum. En Venezuela todas las operadoras de telefonía móvil utilizan los equipos SMSC fabricados por la compañía Logica CMG y usan como estándar la versión del protocolo SMPP ver.3.4.

3.3.2. Visión general del protocolo SMPP

Usando el protocolo SMPP y una aplicación para el manejo de SMS, llamada ESME (*External Short Message Entity*), se puede iniciar una conexión en la capa de aplicación con un SMSC sobre una conexión TCP/IP o X.25 que puede enviar y recibir mensajes a y desde el SMSC respectivo.

El protocolo SMPP soporta un conjunto características de procesamiento en ambos sentidos tales como:

(a) La transmisión de mensajes desde un ESME a uno o múltiples destinos a través del SMSC.
(b) Un ESME puede recibir mensajes a través del SMSC desde otros SME (por ejemplo un móvil, un módem u otro dispositivo capaz de enviar mensajes).
(c) Solicitud del estatus de un mensaje almacenado en el SMSC.
(d) Cancelo o reemplazo de mensajes cortos almacenados en el SMSC.
(e) Envío de mensaje de acuse de recibido (se devuelve un mensaje de notificación de que se recibió el SMS a través del SMSC a quien originó el SMS).
(f) Permite programar la fecha y hora de envío del mensaje.

(g) Seleccionar el modo del mensaje.
(h) Permite establecer prioridad de envío al mensaje
(i) Define el tipo de codificación de los datos del SMS.
(j) Permite establecer el período de validez del SMS.
(k) Asocia tipo de servicios con cada mensaje.

3.3.3. Definición del protocolo SMPP

El protocolo SMPP está basado en el intercambio de solicitudes y respuestas de PDUs (*Protocol Data Unit*) entre el ESME y el SMSC bajo una conexión TCP/IP o X.25.

El protocolo SMPP define:

(a) Un conjunto de operaciones para el intercambio de mensajes cortos entre un ESME y un SMSC.
(b) Los datos que una aplicación tipo ESME debe intercambiar con un SMSC durante las operaciones SMPP.

El intercambio de mensajes entre un ESME y un SMSC vía SMPP se puede categorizar en tres diferentes grupos:

(a) Mensajes enviados desde el *ESME Transmitter* (Transmisor) al SMSC.
(b) Mensajes enviados desde el SMSC al *ESME Receiver* (Receptor).
(c) Mensajes enviados desde el *ESME Transceiver* (Transmisor/Receptor) al SMSC y mensajes enviados desde el SMSC al ESME Transceiver (Transmisor/Receptor).

En la siguiente figura se muestran las categorías antes mencionadas, de las cuales sólo se describirá más adelante la sesión *ESME Transceiver* por ser la empleada en el desarrollo del programa de conexión dedicada al servidor de mensajes cortos de texto SMSC.

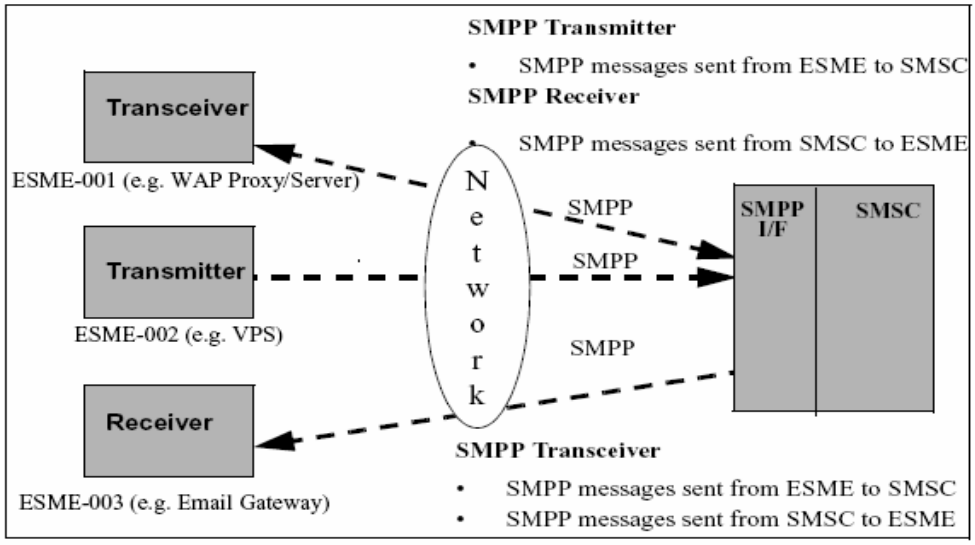

Figura 3.2. Interfaz SMPP entre un SMSC y el ESME [4]

3.3.4. Descripción de la sesión SMPP

Una sesión SMPP entre un SMSC y un ESME es inicializada por el ESME, primero estableciendo una conexión con el SMSC y enviando una solicitud de enlace SMPP (Bind request) para abrir una sesión SMPP. Un ESME que desee enviar y recibir mensajes debe establecer dos conexiones (TCP/IP o X.25) y dos sesiones SMPP (Transmisor y Receptor). Alternativamente en esta versión del protocolo un ESME puede establecer una sesión SMPP transmisor/receptor sobre una conexión única.

Durante una sesión SMPP un ESME puede emitir una serie de solicitudes a un SMSC y podría recibir las respuestas apropiadas de cada solicitud desde el SMSC. Sin embargo el SMSC puede enviar solicitudes al ESME, las cuales debe responder en concordancia a las solicitudes realizadas.

La sesión SMPP puede ser definida en términos de los siguientes posibles estados:

[4] SMPP Forum. Short Message Peer to Peer Protocol Specification v3.4. [2]

(a) OPEN (Conectado y pendiente por enlace).

Un ESME ha establecido una conexión a el SMSC pero aún no ha emitido la solicitud de enlace (*Bind request*).

(b) BOUND_TX

Un ESME conectado al SMSC que ha enviado una solicitud para conectarse como un ESME Transmitter (enviando un *bind_transmitter* PDU) debe recibir una respuesta desde el SMSC autorizando este *bind request*.

Un ESME conectado como *Transmitter* puede enviar mensajes cortos a un SMSC para que sean entregados a un móvil o a otro ESME. El ESME puede también reemplazar, colocar en cola o cancelar un mensaje previamente enviado.

(c) BOUND_RX

Un ESME conectado al SMSC que ha enviado una solicitud para conectarse como un *ESME Receiver* (enviando un *bind_receiver* PDU) debe recibir una respuesta desde el SMSC autorizando este *bind request*.

Un ESME conectado como Receiver puede recibir mensajes cortos desde un SMSC el cual puede ser originado por un móvil u otro ESME o por el SMSC propiamente (por ejemplo un despacho de SMS recibidos por el SMSC).

(d) BOUND_TRX

Un ESME conectado al SMSC que ha enviado una solicitud para conectarse como un *ESME Transceiver* (enviando un *bind_transceiver* PDU) debe recibir una respuesta desde el SMSC autorizando este *bind request*. Un ESME conectado como *Transceiver* soporta el conjunto completo de operaciones soportados por un *ESME Transmitter* y un *ESME Receiver*.

Un ESME conectado de esta manera puede enviar mensajes a un SMSC para que sean entregados a un móvil o a otro ESME. Este también puede recibir mensajes cortos de un SMSC, el cual pudo ser originado por un móvil, por otro ESME o por el propio SMSC.

(e) CLOSED (Desenlazar y desconectarse)

Un ESME se ha desenlazado del SMSC y ha cerrado la conexión. El SMSC también puede desenlazar del ESME.

3.3.5. Outbind

El propósito de la operación *outbind* es permitir que la señal originada por el SMSC al ESME, haga que este emita una solicitud para conectarse como *bind_receiver* al SMSC. Un ejemplo de donde puede ser aplicado, puede ser donde el SMSC consigue un mensaje para entregar a un ESME que está desenlazado.

Una sesión SMPP *outbind* entre el SMSC y el ESME puede ser inicializada por el SMSC primeramente estableciendo una conexión con el ESME. Una vez se ha establecido la conexión, el SMSC podría enlazar al ESME emitiendo una petición "*outbind*". El ESME debe responder con una solicitud "*bind_receiver*" con lo cual el SMSC debe emitir un "*bind_receiver_resp*". Si el ESME no acepta la sesión *outbind* (por ejemplo, debido a un *system_id* o *password* ilegal, etc.) el ESME debe desconectar la conexión.

Una vez la sesión SMPP está establecida, las características de la sesión son las de una sesión normal como SMPP *Receiver*. En la figura 3.3 se muestra el esquema de la secuencia *outbind*.

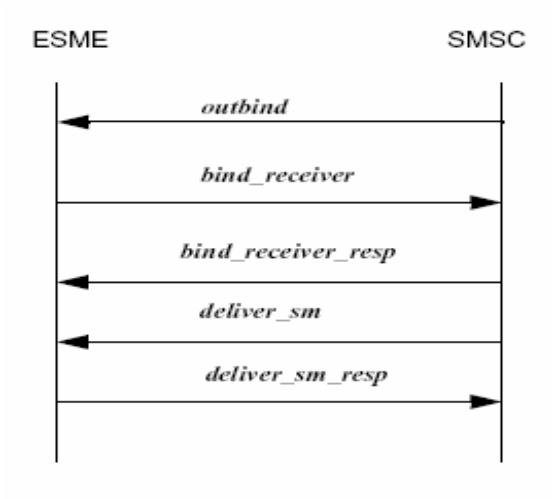

Figura 3.3. Esquema de una sesión *outbind* [5]

[5] SMPP Forum. Short Message Peer to Peer Protocol Specification v3.4. [2]

3.3.6. SMPP PDUs

La siguiente tabla lista el conjunto de SMPP PDU y el contexto en el cual cada PDU puede ser utilizado.

Nombre del SMPP PDU	Estado requerido de la sesión SMPP	Emitido por el ESME	Emitido por el SMSC
Bind_transmitter	**OPEN**	**Yes**	**No**
Bind_transmitter_resp	**OPEN**	**No**	**Yes**
Bind_receiver	**OPEN**	**Yes**	**No**
Bind_receiver_resp	**OPEN**	**No**	**Yes**
Bind_transceiver	**OPEN**	**Yes**	**No**
Bind_transceiver_resp	**OPEN**	**No**	**Yes**
outbind	**OPEN**	**No**	**Yes**
unbind	**BOUND_TX** **BOUND_RX** **BOUND_TRX**	**Yes** **Yes** **Yes**	**Yes** **Yes** **Yes**
unbind_resp	**BOUND_TX** **BOUND_RX** **BOUND_TRX**	**Yes** **Yes** **Yes**	**Yes** **Yes** **Yes**
submit_sm	**BOUND_TX** **BOUND_TRX**	**Yes** **Yes**	**No** **No**
submit_sm_resp	**BOUND_TX** **BOUND_TRX**	**No** **No**	**Yes** **Yes**
submit_sm_multi	**BOUND_TX** **BOUND_TRX**	**Yes** **Yes**	**No** **No**
submit_sm_multi_resp	**BOUND_TX** **BOUND_TRX**	**No** **No**	**Yes** **Yes**
Data_sm	**BOUND_TX** **BOUND_RX** **BOUND_TRX**	**Yes** **Yes** **Yes**	**Yes** **Yes** **Yes**
Data_sm_resp	**BOUND_TX** **BOUND_RX** **BOUND_TRX**	**Yes** **Yes** **Yes**	**Yes** **Yes** **Yes**
deliver_sm	**BOUND_RX** **BOUND_TRX**	**No** **No**	**Yes** **Yes**
deliver_sm_resp	**BOUND_RX** **BOUND_TRX**	**Yes** **Yes**	**No** **No**

Quero_sm	**BOUND_TX** **BOUND_TRX**	**Yes** **Yes**	**No** **No**
Quero_sm_resp	**BOUND_TX** **BOUND_TRX**	**No** **No**	**Yes** **Yes**
cancel_sm	**BOUND_TX** **BOUND_TRX**	**Yes** **Yes**	**No** **No**
cancel_sm_resp	**BOUND_TX** **BOUND_TRX**	**No** **No**	**Yes** **Yes**
replace_sm	**BOUND_TX**	**Yes**	**No**
replace_sm_resp	**BOUND_TX**	**No**	**Yes**
enquire_link	**BOUND_TX** **BOUND_RX** **BOUND_TRX**	**Yes** **Yes** **Yes**	**Yes** **Yes** **Yes**
enquire_link_resp	**BOUND_TX** **BOUND_RX** **BOUND_TRX**	**Yes** **Yes** **Yes**	**Yes** **Yes** **Yes**
Alert_notification	**BOUND_RX** **BOUND_TRX**	**No** **No**	**Yes** **Yes**
generic_nack	**BOUND_TX** **BOUND_RX** **BOUND_TRX**	**Yes** **Yes** **Yes**	**Yes** **Yes** **Yes**

Tabla 3.1 SMPP PDU para las diferentes sesiones SMPP

3.3.7. Capa de conexión SMPP

La interfaz de transporte entre un ESME y un SMSC puede estar basada en una conexión de red TCP/IP o X.25.

SMPP es un protocolo en la capa de aplicación que no intenta ofrecer funcionalidades de transporte. Por consiguiente esto es asumido por las capas más bajas de la conexión de red, las cuales proveen la confiabilidad de la transferencia de datos punto a punto incluyendo codificación de paquetes, control de flujo y manejo de errores. Una vez que se transfiere la confiabilidad de transporte a capas inferiores, en el nivel SMPP el ESME y el SMSC deben tratar la conexión como un transporte fiable el cual envía y recibe SMPP PDUs.

En la figura 3.4 se ilustra la implementación de una interfaz genérica entre un ESME y un SMSC.

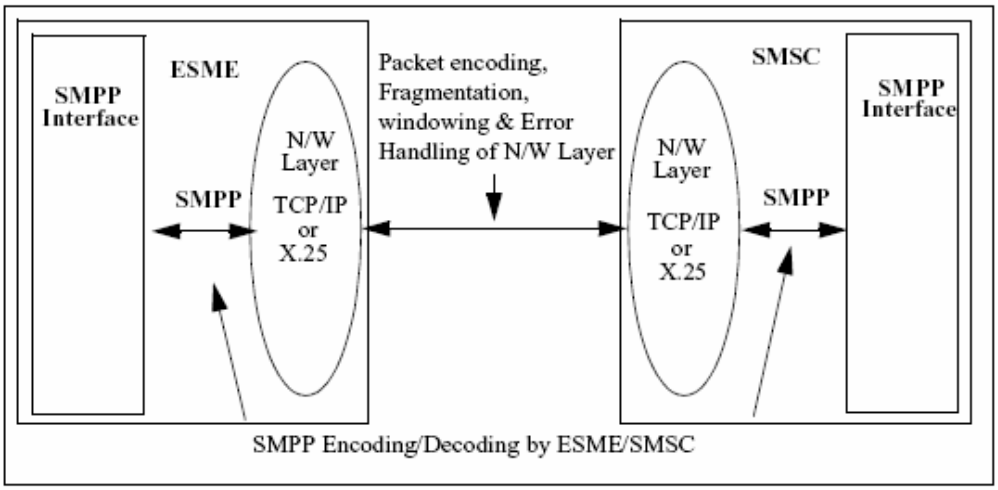

Figura 3.4. Modelo de una interfaz SMPP SMSC-ESME [6]

3.3.8. Intercambio de mensajes en ambos sentidos entre un SMSC y un ESME

El SMSC y ESME pueden interactuar en una sesión para intercambio de mensajes bidireccionales. En este caso el ESME debe estar conectado al SMSC como un *ESME Transceiver*.

Aplicaciones típicas en las cuales un ESME podría operar como un SMPP *Transceiver* incluyen:

(a) Intercambio de mensajes en ambos sentidos entre un móvil y un ESME, como por ejemplo un WAP Proxy Server. El suscriptor móvil inicia la petición de información al WAP Proxy Server y la información de respuesta es devuelta vía el SMSC al suscriptor móvil.

[6] SMPP Forum. Short Message Peer to Peer Protocol Specification v3.4. [2]

Ejemplos de mensajes SMPP PDUs los cuales podrían ser enviados en una sesión SMPP Transceiver incluyen:

(a) ***data_sm***
(b) ***submit_sm***
(c) ***deliver_sm***

Además del envío de mensajes al SMSC, un ESME puede llevar acabo las siguientes operaciones SMPP usando el identificador de mensajes devuelto por el SMSC en los mensajes de reconocimiento:

(a) ***query_sm.*** Se solicita al SMSC el estatus de un mensaje que fue previamente enviado.
(b) ***replace_sm.*** Remplaza un mensaje que fue enviado.
(c) ***cancel_sm.*** Cancela el envío por parte del SMSC de un mensaje enviado.

Los SMPP PDUs enviados a un ESME por el SMSC (o viceversa) deben ser reconocidos y debe devolverse el PDU de respuesta correspondiente cuando son recibidos. La única excepción a esta regla es cuando se emite el PDU de notificación de alerta (*alert_notification*).

3.3.9. Secuencia típica de una sesión SMPP ESME Transceiver

El siguiente diagrama ilustra una secuencia típica SMPP *request/response* entre un SMSC y un ESME conectado como *Transceiver*.

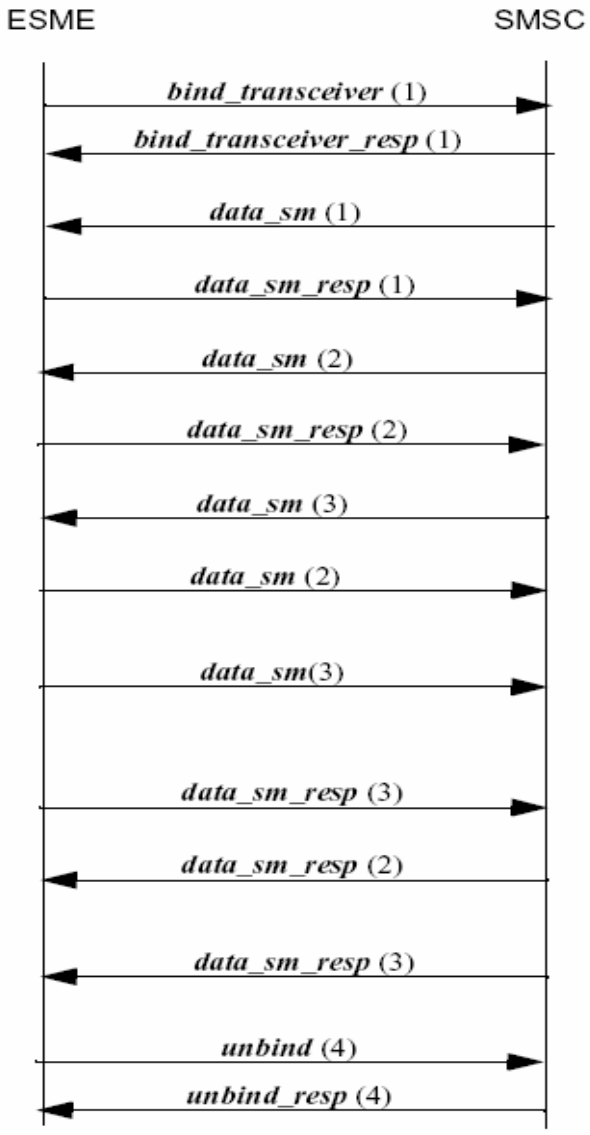

Figura 3.5. Secuencia típica SMPP *request/response* para un ESME conectado *Transceiver* [7]

(a) El intercambio de SMPP PDUs del tipo *request* y response entre un SMSC y un ESME *Transceiver* puede ser implementado tanto de manera sincrónica como asincrónica como se muestra en la figura 3.5. De esta manera el SMSC puede enviar múltiples solicitudes del tipo *data_sm* al

[7] SMPP Forum. Short Message Peer to Peer Protocol Specification v3.4. [2]

ESME, sin la necesidad de esperar de manera sincronizada la respuesta asociada al PDU (*data_sm_resp*) enviado.

(b) Una serie de sucesivos SMPP PDUs del tipo *request* emitidos de manera asincrónica por un SMSC (como se ve en la figura 3.5 y se denota por el número entre paréntesis) deben ser seguidos luego por unas series de respuesta asociadas desde el ESME. El parámetro *sequence_number* en el SMPP *header* es usado para correlacionar el SMPP response PDU, con SMPP request PDU enviado.

(c) El ESME podría siempre devolver la respuesta del SMPP PDU al SMSC en el mismo orden en cual las solicitudes fueron recibidas. Sin embargo esto no es obligatorio en el protocolo SMPP, y el SMSC debe ser capaz de manejar las respuestas recibidas fuera de secuencia.

(d) Los SMPP responses podrían ser devueltos por el SMSC en el mismo orden en el cual fueron recibidas las solicitudes originales desde el ESME. Sin embargo esto no es obligatorio en el protocolo SMPP, y el SMSC debe ser capaz de manejar las respuestas recibidas fuera de secuencia.

El número máximo operaciones SMPP entre un ESME y un SMSC y viceversa, no están explícitamente especificadas en la especificación del protocolo SMPP y podría ser manejado por el SMPP implementado en el SMSC. Sin embargo se recomienda que no sean más de diez mensajes SMPP.

3.4. Desarrollo del programa de conexión dedicada al SMSC

Una vez descrito el protocolo de comunicación utilizado para la comunicación entre el SMSC y el ESME, el cual es el SMPP v3.4 (*Short Message Peer to Peer*) y el cual es el que actualmente utilizan las operadoras de telefonía celular en Venezuela, se describirá el desarrollo del programa para la conexión al servidor o centro de mensajes cortos SMSC.

Este programa permitirá establecer la conexión dedicada al SMSC y a través de este se podrán enviar y recibir los datos que harán posible el desarrollo de la plataforma para servicios basados en localización.

Más adelante se establecerán los parámetros que serán enviados en los SMS al SMSC, para que este los remita el ESME correspondiente y puedan ser manejados y procesados acorde al tipo de tratamiento que se le deba realizar según la solicitud del usuario que hizo la petición.

3.4.1. Lenguaje de programación usado para el diseño del programa de conexión dedicada al SMSC

El lenguaje de programación elegido para el diseño del programa de conexión dedicada al SMSC es Java. Java es un lenguaje es orientado a objetos, eso implica que su concepción es muy próxima a la forma de pensar humana. La sintaxis de este programa es muy similar a la usada por C++. Además java es un lenguaje multiplataforma, lo que quiere decir que el código java que funciona en un sistema operativo funcionará en cualquier otro sistema operativo que posea instalada la máquina virtual de java.

Gracias a los API (Application Programming Interface) de java podemos ampliar el lenguaje para que sea capaz de, por ejemplo, comunicarse con equipos mediante redes, acceder a bases de datos, crear páginas HTML dinámicas, crear aplicaciones visuales al estilo Windows, entre otros conjuntos de aplicaciones.

Para poder trabajar con java es necesario emplear un software que permita desarrollar en java. Existen varias alternativas comerciales en el mercado como: JBuilder, Visual Age, Visual Café, JCreator, etc.

Una de las características que hace atractivo el uso de java es que el lenguaje es software libre, es decir no tiene costo alguno. Por eso su uso es de gran

demanda en aplicaciones corporativas donde se busca abaratar los costos de desarrollo.

3.4.2. Descripción del programa desarrollado

El programa fue desarrollado según los requerimientos estándar que necesitan las aplicaciones tipo ESME, para la transmisión y recepción de mensajes cortos en la red de telefonía celular de Digitel TIM.

En primera instancia el programa desarrollado debe crear una conexión TCP/IP con el SMSC de Digitel a través de la plataforma MAR (Message Application Router), cuyo fabricante es Logica CMG. Esta conexión TCP/IP como se mencionó antes, provee la capa de transporte donde se insertarán los comandos y parámetros del protocolo SMPP.

Para esto se utilizó una clase de java que maneja sesiones TCP/IP, claro que para iniciar una conexión de este tipo debemos saber el puerto y la dirección IP donde deseamos iniciar la sesión. Para el desarrollo del proyecto los parámetros establecidos fueron:

(a) Dirección IP o Mar Nodel: 10.26.2.45
(b) Puerto TCP: 17600

Una vez iniciada la sesión TCP/IP, esta servirá como capa de transporte confiable para que sobre ella se monte el protocolo SMPP en la capa de aplicación. Esta conexión se hace a un puerto y dirección IP específica en la MAR de Digitel, sin que aún se haya establecido una conexión para el envío y recepción de mensajes cortos, como las mencionadas en las secciones anteriores.

Una vez establecida la conexión que servirá de transporte para el envío y recepción de los SMPP PDUs, se utilizó un API de java para el manejo del protocolo SMPP entre el SMSC y el ESME propiamente dicho.

A este API se le configuraron ciertos parámetros que permiten que se establezcan conexiones directas con el SMSC desde el ESME, y se puedan iniciar transacciones para el envío y recepción de SMS.

Dichos parámetros fueron:

(a) *System_ID*: lbs
(b) *System_Type*: smpp
(c) *Password*: lbs99

El parámetro *System_ID* es usado para identificar al ESME en el momento de iniciar el enlace, el *Password* es usado por el SMSC para autenticar la identidad del ESME que desea conectarse y el *System_Type* es usado para categorizar al ESME que desea conectarse con el SMSC.

Estos parámetros son enviados en las peticiones solicitada por el ESME al SMSC para conectarse en cualquiera de los modos de conexión antes descritos; es decir como *bind_receiver*, *bind_transmitter* o *bind_transceiver*. En el desarrollo se utilizó el *bind_transceiver* como el modo de conexión para el intercambio de paquetes entre el ESME y el SMSC, debido a que con una sola sesión se pueden manejar tanto la recepción como el envío de SMS.

Cuando se le hace una solicitud de conexión al SMSC desde el ESME para conectarse como *transceiver* obligatoriamente deben enviarse los parámetros antes mencionados. Estos parámetros se guardaron en un archivo de configuración que es leído cada vez que se quiere iniciar una conexión.

Una vez enviados estos parámetros en una solicitud del tipo *bind*, a través del programa de conexión dedicada y éstos han sido autenticados desde el SMSC, ya se pueden enviar y recibir mensajes de texto, en otras palabras se pueden iniciar transacciones de SMS en ambos sentidos.

CAPÍTULO IV

MÉTODO Y PROGRAMA PARA PROCESAMIENTO DE UBICACIÓN

4.1. Fundamentos y métodos de localización existentes hoy en día

Los métodos que se describirán a continuación están basados tecnología para redes celulares. Determinados métodos de los que se proponen en la actualidad se pueden desarrollar directamente mientras que otros requieren modificaciones a nivel de la red y en algunos casos modificaciones a nivel del móvil.

Los métodos de localización que se describirán son:

(a) Técnicas basadas en la identidad de la celda que da cobertura al móvil

- Identidad de la celda que da cobertura al móvil (Cell Identity, CI)
- Identidad de la celda que da cobertura al móvil mejorada (Enhanced Cell Identity, ECI)

(b) Técnicas basadas en la red

- Ángulo de llegada (Angle of Arrival, AOA)
- Tiempo de llegada (Time of Arrival, TOA)
- Diferencia en el tiempo de llegada (Time Difference of Arrival, TDOA)

(c) Técnicas basadas en la modificación del móvil

- Diferencia en el tiempo de llegada con Terminal modificado (TOA)
- Diferencia en el tiempo de llegada perfeccionado (Enhanced Observe Time Difference, E-OTD)
- Triangulación avanzada de enlace hacia delante (Advanced Forward Link Trilateration, A-FLT)
- Sistema de posicionamiento global avanzado (Global Positioning System, GPS, A-GPS)

4.1.1. Técnicas basadas en la identidad de la celda que da cobertura al móvil

Las técnicas basadas en la identidad de la celda que le presta servicio al móvil se pueden desplegar sin la necesidad de realizar inversiones, cambios o modificaciones en las redes celulares actuales, como en el caso de redes GSM. La estimación de la posición de un móvil se puede obtener mediante la obtención de la identidad de la celda que en ese momento le da cobertura, debido a que al conocer la posición geográfica donde se encuentra la celda; se conoce de cierta manera la posición del móvil. Con esta técnica se pueden localizar dispositivos móviles en redes celulares como GSM, GPRS, UMTS y CDMA.

Además de obtener el CI de la celda que le da cobertura al móvil, el cual es el parámetro que identifica la celda que presta servicio; el método se puede perfeccionar tomando en cuenta dos parámetros adicionales: El TA (Timing Advance) y el NMR (Network Measurement Result). El TA es el parámetro de avance temporal para transmitir sobre el canal de radio y el NMR es el resultado de las mediciones realizadas en la red. El tomar en cuenta todos estos parámetros para intentar estimar la posición hace que el método se convierta en ECI (Enhanced Cell Identity)

El CI identifica de manera única la celda en la que se encuentra registrado el móvil, mientras que el TA indica la distancia a la cual se encuentra el móvil de la estación; este parámetro se utiliza en GSM para indicarle al móvil en qué momento debe iniciar la transmisión para que los datos sean insertados en el “time slot” asignado para la comunicación con la radio base. Este parámetro nos da una idea de la distancia a la cual se encuentra el móvil de la radio base. Además de tener el parámetro del TA para estimar la posición del móvil tenemos el NMR el cual contiene los resultados de las mediciones realizadas en las celdas vecinas y la servidora. Este reporte contiene los niveles de potencia de las celdas como su identificación. Una vez recolectados estos parámetros se pueden aplicar técnicas de triangulación para determinar la posición del móvil.

El grado de exactitud que puedan presentar estos métodos va a depender del tipo de zona donde se encuentre el usuario, es decir; si la zona es urbana o rural. Si la zona es urbana generalmente las celdas son de pequeña cobertura, desde 200 metros hasta escasos kilómetros. En áreas rurales las celdas son capaces de cubrir hasta 35 Km en línea de vista. Por lo antes mencionado, la precisión del método va a depender del tipo de zona donde se encuentre el móvil. Generalmente la precisión alcanzada con este método no es tan alta, va desde los 50 metros hasta cientos de metros en zonas urbanas y unidades de kilómetros en zonas rurales; pero a la hora de ofrecer servicios basados en localización en entornos urbanos con penetración inmediata, es uno de los métodos más utilizados por los operadores de redes celulares.

4.1.2. Técnicas basadas en la red

Para el despliegue de técnicas o métodos que se basan en la red para estimar la posición del móvil, se requiere que se realicen modificaciones a nivel de hardware en las redes, así como la colocación de equipos especiales que permitirán calcular la posición. Estas técnicas que se verán a continuación impactan a nivel económico a los operadores que deseen desplegar una infraestructura de localización de este tipo, debido la inserción de nuevos equipos que deben ser colocados en la red. Esta técnica garantiza una mejor precisión pero requiere de inversión y modificaciones para su desarrollo.

(a) Ángulo de llegada (Angle of Arrival, AOA)

Esta técnica hace uso de arreglos especiales de antenas que son colocados en las radio bases de las redes celulares donde se desea implementar esta técnica de localización. La técnica consiste en determinar el ángulo de la señal incidente que es emitida por el móvil a los arreglos de antenas situados en las radio bases, solo si existe línea de vista LOS (Line of Sight). Si existe la línea de vista el arreglo de antenas puede determinar la dirección de donde procede la señal transmitida, pero

para conocer con mejor exactitud la posición hace falta una segunda radio base con un arreglo de antenas similar al primero y que sea capaz de estimar la segunda posición. Una vez estimadas las posibles localizaciones la segunda estación que realizó el cálculo tratará de ubicar al móvil comparando sus datos con los de la primera estación que realizó los cálculos, para luego determinar por cálculos trigonométricos la ubicación del móvil.

Debido a que el método requiere de línea de vista entre el móvil y el arreglo de antenas en la radio base, este resulta más efectivo en entornos rurales donde en la mayoría de los casos se tiene línea de vista, y sólo se necesitan dos radio base para el cálculo de la posición. En entornos urbanos es necesario emplear más de dos estaciones para estimar la ubicación, debido a que en muchos casos se carece de línea de vista entre el móvil y la radio base, y por ende se comete un mayor error al realizar la estimación de localización.

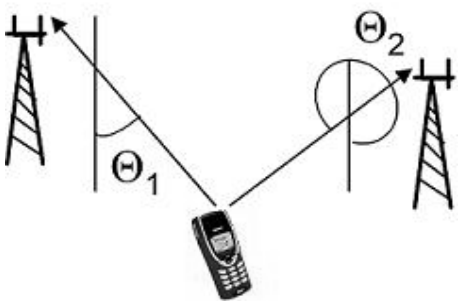

Figura 4.1. Sistema de localización por ángulo de llegada [8]

(b) Tiempo de llegada (Time of Arrival, TOA)

La técnica consiste en medir el tiempo que tarda en llegar una señal que es enviada por el móvil a un conjunto de radio bases. Esto consiste en capturar el tiempo que tarda en llegar la señal a las radio bases y regresar hasta el móvil. La distancia se puede calcular asumiendo que la señal viaja a la velocidad de la luz y

[8] Fuente: http://www.ceditec.etsit.upm.es/localizacion.php

multiplicando este valor por el tiempo calculado; esto nos da como resultado la distancia a la que se encuentra el móvil de la radio base.

Para emplear este método es necesario obtener la medición de al menos tres radio bases, debido a que se deben emplear técnicas de triangulación para calcular la posición del móvil. Con las distancias calculadas respecto a las radio bases se pueden describir circunferencias cuyos centros se encuentran en ellas, la posición del móvil es el resultado de la intersección de dichas circunferencias. Los datos de las distancias del móvil a las radio bases son enviados a un servidor que se encarga de procesarlos y corregir los posibles errores aplicando métodos matemáticos.

Una desventaja que posee el método es que la ausencia de línea de vista entre el móvil y la radio base puede introducir errores al estimar el tiempo que tarda en ir y regresar la señal debido a los rebotes con diferentes obstáculos en su recorrido. Estos errores causan estimaciones erróneas de localización.

(c) Diferencia en el tiempo de llegada (Time Difference of Arrival, TDOA)

Según Bernados el método TDOA emplea la diferencia entre los tiempos de llegada de la señal procedente del terminal móvil a distintos pares de estaciones base para calcular la posición. Puesto que la curva cuyos puntos satisfacen la condición de que su distancia a dos referencias (en este caso un par de radio base) sea una constante es una hipérbola, si se calcula esta correlación para varios pares de estaciones base la intersección de las hipérbolas resultantes muestra el punto donde se encuentra el móvil. [6]

Una ventaja que presenta ese método con respecto al método TOA es que este funciona sin que exista línea de vista entre la radio base y el móvil debido a que la diferencia de tiempo elimina los errores que se pudiesen introducir por las reflexiones o rebotes de la señal al encontrar obstáculos en su recorrido. Pero se

debe tomar en cuenta que para zonas donde exista la presencia de muchos obstáculos como edificios, es decir; zonas del tipo urbano, se hace necesario el realizar la estimación de la posición respecto a cuatro radio bases para tener una mejor precisión y reducir los errores que traen consigo las múltiples reflexiones.

En ambientes abiertos o rurales esta técnica se puede combinar con la AOA para proporcionar mayor precisión. En la figura 4.2 se muestra el método antes descrito.

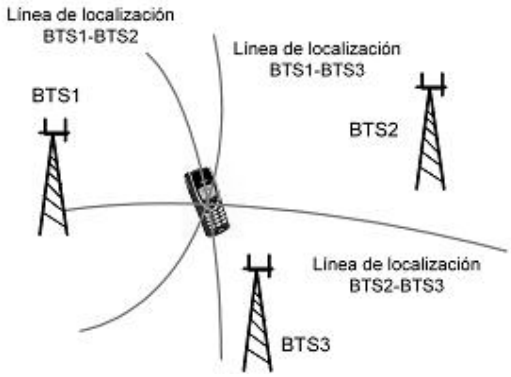

Figura 4.2. Sistema de localización TDOA [9]

4.1.3. Técnicas basadas en la modificación del móvil

(a) Diferencia en el tiempo de llegada con Terminal modificado (TOA)

Esta técnica basada en la modificación del móvil se fundamenta en el mismo principio del método TOA mencionado antes pero en este caso el móvil es capaz de determinar el instante en el cual se genera la señal que se le envían al conjunto de radio bases mediante marcas temporales. Al igual que el método TOA se necesitan al menos tres radio bases para poder estimar la ubicación del móvil.

[9] Fuente: http://www.ceditec.etsit.upm.es/localizacion.php

De acuerdo a Bernados la desventaja de este método, y lo que lo hace realmente complejo y caro, es que requiere que las estaciones base y el móvil tengan relojes precisos y sincronizados. [6]

(b) Diferencia en el tiempo de llegada perfeccionado (Enhanced Observe Time Difference, E-OTD)

Según el documento de Bernados, la técnica E-OTD opera sobre redes GSM y GPRS e incluye nueva tecnología tanto en el móvil como en la red. Siendo la solución de red similar a la utilizada en TDOA, el sistema necesita que se instalen unidades de medida de posición (Location Measurement Units, LMU) a modo de balizas de referencia en puntos dispersos geográficamente. La densidad de LMUs determinará la precisión del sistema, y por ello normalmente es necesario instalar en toda la red una LMU por cada una o dos estaciones base. Estos receptores y los terminales móviles habilitados con software E-OTD realizan medidas de las señales procedentes de tres o más estaciones base periódicamente. Las diferencias temporales de llegada de la señal a los dos puntos (LMU y terminal) se combinan para producir líneas hiperbólicas que se intersecan en el lugar donde está el móvil, ofreciendo de esta manera localización en dos dimensiones. [6]

Esta técnica que se fundamenta en la modificación del móvil consiste en hacer que el equipo mida la diferencia en tiempo que tardan en llegar los datos enviados por dos radio bases cercanas al mismo. En este caso se debe garantizar que las estaciones estén sincronizadas, pero en el caso de que no lo estén como ocurre en redes GSM, se debe monitorear el posible desfase que puede existir entre ellas para poder calcular las diferencias de tiempo reales (Relative Time Difference - RTD).

Para garantizar una buena precisión se recomienda las mediciones de al menos tres radio bases, para así poseer las mediciones del tiempo de diferencia observado y la diferencia de tiempo relativo, una vez que se obtienen los

resultados de las mediciones existen dos maneras de calcular la ubicación del móvil, bien sea asistido por red o asistido por el móvil. En el primer caso (asistido por red) el móvil mide el OTD y la red se encarga de suministrar las coordenadas de la estación y el RTD al móvil para que este estime la posición. En el segundo caso (asistido por el móvil), es el equipo el encargado de suministrarle a la red el valor del OTD correspondiente a las estaciones monitoreadas para que esta estime la posición. De cualquier manera que se quiera implementar el método, sea asistido por la red o por el móvil, la posición se debe calcular mediante triangulación con los datos obtenidos en las mediciones, es decir; el OTD, el RTD y las coordenadas de las estaciones.

(c) Triangulación avanzada de enlace hacia delante (Advanced Forward Link Trilateration, A-FLT)

Este método es muy similar al TDOA y por ende su funcionamiento es básicamente el mismo y consiste en realizar las mediciones del retardo de la fase que existe entre las señales que les son enviadas a un par de radio bases y realizar una comparación con las mediciones realizadas en otro par de radio bases. Cabe destacar que esta técnica es de uso exclusivo para redes CDMA debido a la sincronía que estas presentan y a que el método requiere que las estaciones se encuentren sincronizadas. Al igual que TDOA, para estimar la ubicación del móvil hace falta la información de al menos tres radio bases. Aparte de esta técnica existe una mejora que se fundamenta en los mismos criterios de A-FLT, llamada EFLT (Enhanced Forward Link Trilateration).

(d) Sistema de posicionamiento global avanzado (Global Positioning System, GPS, A-GPS)

Según Bernados la asistencia que este sistema proporciona respecto al GPS tradicional radica en el uso de receptores de referencia. Estos receptores recogen información de navegación y datos de corrección diferencial para los satélites

GPS que están en la zona de cobertura del servidor de localización. A partir de la información obtenida, el servidor de localización facilita bajo demanda datos de interés a los terminales móviles, principalmente una lista con las efemérides de los satélites (órbitas recalculadas con los datos de corrección suministrados por las estaciones de tierra) visibles para el móvil. Los datos, que se introducen en un pequeño mensaje de unos 50 bytes, son todo lo que el móvil necesita saber para completar los datos GPS recibidos. El servidor de localización puede también tener acceso a una base de datos de elevaciones del terreno que permite precisar la altitud a la que se encuentra el móvil, efectuando de esta manera una localización en tres dimensiones. [6]

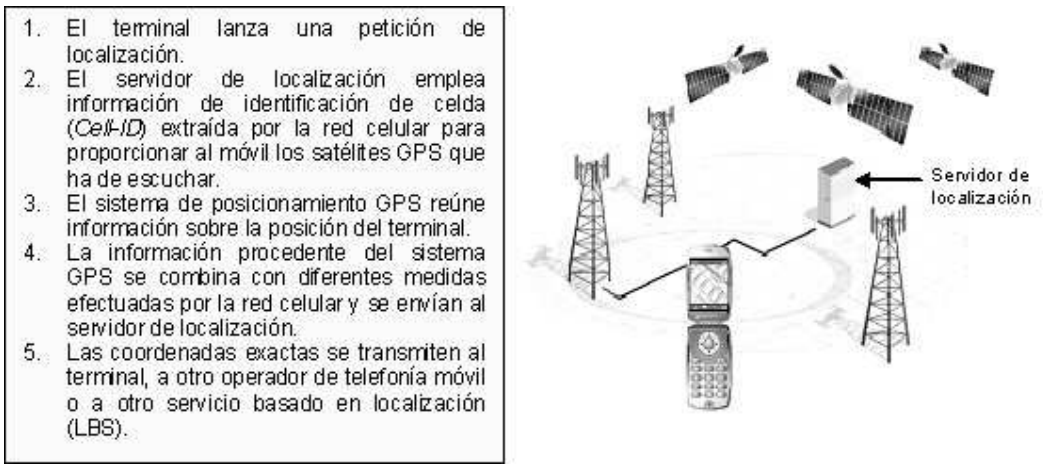

Figura 4.3. Sistema de localización A-GPS y Cell Identity [10]

Mediante este método se le proporciona al móvil provisto de un GPS, los satélites que se encuentran en la zona de interés para que éste los tome como referencia a la hora de realizar las estimaciones, además de datos para la corrección de las mediciones realizadas. Con estos parámetros se reduce el margen de error cometido al calcular las coordenadas geográficas mediante el GPS. En la figura 4.8 se puede observar el proceso de localización mediante la técnica A-GPS.

[10] Fuente: http://www.ceditec.etsit.upm.es/localizacion.php

Debido a que esta solución hace uso del GPS para el cálculo de la posición, es posible usarla tanto en redes síncronas (CDMA) como asíncronas (GSM, GPRS y UMTS). El único problema que se presenta en este tipo de técnica es el error que se comete al no poseer línea de vista con los satélites por obstrucciones ocasionadas por edificaciones o zonas de mucho follaje, del resto es una técnica que garantiza una alta precisión pero con costos elevados a la hora de implementarla.

4.2. Propuesta del método de localización a implementar

El método de localización propuesto se fundamenta en técnicas básicas que utilizan la identidad de la celda que presta cobertura al móvil en el momento que se realiza la solicitud de ubicación, aunque se puede decir que es un método perfeccionado ya que incluye datos que permiten refinar la ubicación del usuario como lo son el NMR (Network Measurement Results) y los datos de la huella cobertura de las estaciones llamados “Drive Test”. Para llevar a cabo la implementación del sistema de localización debemos realizar cambios en el móvil, pero en este caso es a nivel de la SIM, la cual es portable y tiene como ventaja que la aplicación principal de localización sea llevada en ella y no en el equipo terminal.

El método propuesto cotejará datos de la celda que le presta servicio más datos dados por el NMR como: nivel de potencia de la celda servidora y vecinas e identidad de las celdas vecinas a través del BCCH (Broadcast Control Channel) y el BSIC (Base Transceiver Station Identity Code). Conocidos todos estos parámetros y pruebas realizadas se desarrolló un método que fuese capaz de estimar la ubicación del móvil basado en huellas de cobertura de la red. Este método cuenta tanto con los datos de su mejor estación servidora como con los datos de las estaciones vecinas para estimar los cálculos de ubicación.

Como se dijo antes el método de localización contará con dos entes fundamentales para su desarrollo, uno es la SIM y el otro es la aplicación ESME o

Servidor de Aplicaciones; es decir el servidor que contendrá las bases de datos con la información pertinente para estimar el cálculo de la ubicación.

La SIM almacenará el programa encargado de solicitarle al móvil a través del comando STK “Provide Local Information”, la información del estado de las estaciones, está información es vital y crucial para estimar los cálculos de ubicación.

A continuación en la figura 4.5 se muestra el esquema del sistema de localización móvil propuesto y desarrollado.

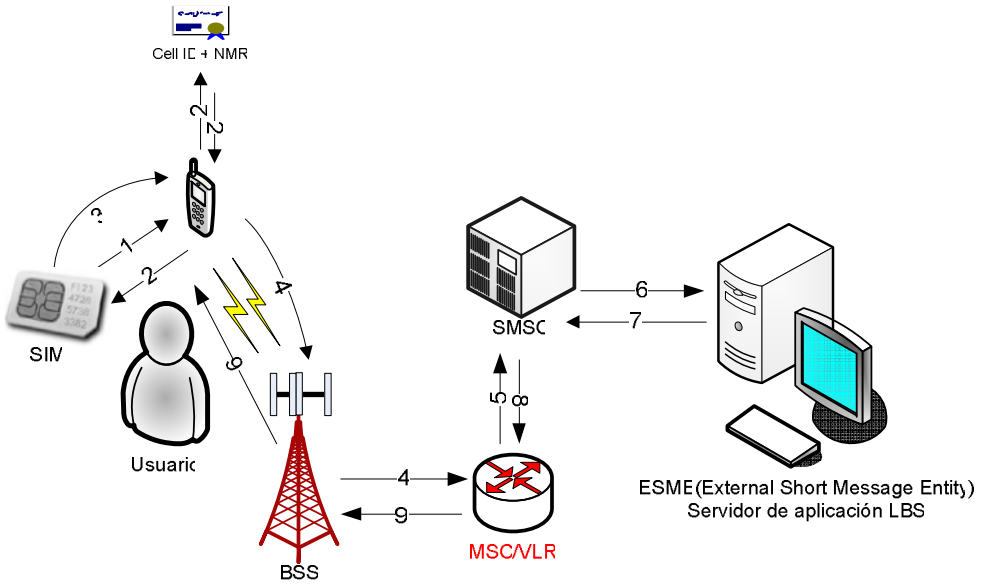

Figura 4.4. Esquema del sistema de localización móvil propuesto

Siguiendo el orden dado en la figura 4.5 el método de localización propuesto se puede describir de la siguiente forma:

- Paso 1. El usuario inicia la solicitud del servicio, lo que hace que se ejecute el programa cargado en la SIM, el cual le envía al móvil el comando STK “Provide Local Information” para que este le devuelva la información solicitada, es decir le devuelva los resultados de las mediciones realizadas por el móvil en la celda servidora y las vecinas.
- Paso 2. El móvil monitorea el estatus de la celda servidora y vecinas, recoge la información solicitada y se prepara para devolverla a la SIM.

- Paso 3. La SIM recibe la información del móvil, la almacena temporalmente, la ordena en un orden previamente establecido y la empaqueta en un SMS con el respectivo identificador del servicio demandado e indicando a que número se enviará. Luego esta información se le pasa al móvil para que este se encargue de enviarla a través de la red.
- Paso 4. El móvil envía la información a través de la red al número especificado.
- Paso 5 y 6. El MSC recibe la solicitud y descifra que es un mensaje de texto, por ser un SMS es enviado al SMSC el cual verifica el destino. Al darse cuenta que es un mensaje para el Servidor de Aplicación LBS o ESME, lo enruta a través de la conexión TCP/IP previamente establecida a dicho servidor de aplicaciones.
- Paso 7. El servidor de aplicaciones procesa la información suministrada, consulta las bases de datos que contienen la información de todas las celdas de la red y ejecuta los cálculos que estimarán la ubicación del móvil. Una vez calculada y estimada la ubicación se realiza otra consulta a la base de datos con el fin de obtener el servicio más cercano a la posición real del usuario. Esta información es devuelta al SMSC junto con el número de destino.
- Paso 8. El SMSC recibe la solicitud de remitir el mensaje enviado por el servidor de aplicaciones. Una vez recibida esta información es enrutada a través del MSC para que sea entregada al número de destino.
- Paso 9. La información enviada por el servidor de aplicaciones es enrutada por el MSC y entregada al móvil que realizó la solicitud. Esta es la respuesta de la solicitud de localización realizada por el usuario.

4.3. Método de localización empleado utilizando como referencia la huella de cobertura “Drive Test” y un método de comparación directo celda a señal

4.3.1. Descripción de los procedimientos, pasos previos y parámetros a ser considerados para el desarrollo del método

En principio este método sale del estudio de pruebas realizadas y por un método muy práctico y laborioso como lo es el método del ensayo y error. Primero se empezó por descifrar los datos solicitados y provistos por el comando STK que envía la SIM al móvil, una vez obtenida se comenzó por comprobar que efectivamente los valores arrojados correspondían con los que efectivamente monitoreaba el móvil en ese momento. Para esto se realizaron una serie de pruebas que consistieron en situarse en zonas donde se conocían con exactitud la identidad de la celda servidora y de las celdas vecinas, una vez allí y apoyado con

una herramienta llamada “Net Monitor”, que es cargada en el móvil y es capaz de permitir la visualización del estado de la red, se verificó que efectivamente los parámetros solicitados al móvil correspondiesen con los datos arrojados por esta herramienta. Una vez corroboradas y analizadas las mediciones, se observó que las pruebas realizadas arrojaron ciertos detalles importantes que deben ser tomados en consideración en el desarrollo del método. Uno de los detalles es que los valores de potencia recibidos están acotados en un rango que va desde -48 dBm ≤ RXLEV ≤ -110 dBm según el estándar GMS 05.08, donde RXLEV es el nivel de recepción recibido por el móvil. Esto trae como consecuencia la limitación en el rango de potencia recibida al solicitarla a través del comando STK, es decir cualquier valor de potencia recibido mayor a -48 dBm será truncado y establecido a -48 dBm, pero se sabe según pruebas realizadas que el móvil es capaz y puede recibir niveles de potencia mayores a dicho valor. Otro detalle importante es que el parámetro BCCH, el cual da el canal de frecuencia de las celdas vecinas, no era obtenido directamente en la primera decodificación. Al realizar la primera decodificación éste arrojaba un valor acotado entre 0 y 32, que a su vez correspondía con el índice de una lista de celdas vecinas definida en la estación servidora como posibles y futuras servidoras a prestar servicios al móvil. Se tiene que a una estación se le pueden configurar hasta 32 posibles vecinas donde el móvil puede realizar handover y que le es suministrada al móvil para su gestión en una lista con un orden determinado.

Para poder descifrar a qué canal de frecuencia correspondía el índice arrojado en el parámetro BCCH se le tuvo que solicitar al móvil que suministrara dicha lista, llamada BCCH channel list y la cual se describe en el estándar GSM 11.14. El BCCH channel list es el parámetro que contiene la lista de canales absolutos de RF para las portadoras de BCCH. Una vez obtenida la información del BCCH channel list y con el valor del parámetro BCCH se pudo obtener el valor del verdadero BCCH, asignando a la lista según en el orden que fue enviada por el móvil, un índice comenzando desde la posición 0 a la 31, para luego cruzarla con la información del índice dado en el BCCH. Una vez realizado el cruce de información podemos conocer los canales de frecuencia de las celdas

vecinas, es decir para el índice obtenido en la vecina-n; qué canal de RF se le asigna en la lista.

Para descifrar el identificador de las celdas vecinas arrojadas por el móvil, o lo que es lo mismo el Cell ID, se necesitó un procesamiento especial del BCCH con el BSIC. Se necesitó información de la configuración de las estaciones en cuanto a la lista de celdas vecinas predefinidas.

En GSM se le pueden definir un máximo de 32 posibles celdas donde el móvil puede conmutar a la hora de requerirlo, como por ejemplo ocurre en el proceso de handover. Esta lista es la que se le envía al teléfono para que sepa a qué celda conmutar a la hora de requerirlo, es ésta la que se carga a las estaciones y es predefinida por los operadores de la red. Obteniendo la lista de todas las celdas vecinas por cada estación se logró obtener el valor del Cell ID asociado a cada celda vecina, conectando a una base de datos donde se encontraban dichos valores y realizando una consulta que relacionaba el BCCH y el BSIC para poder obtener el valor del Cell ID asociado a dichos parámetros. Una vez conocidos los Cell ID se sabe a cabalidad toda la información relacionada con cada celda vecina y estos pueden ser empleados para realizar los cálculos de ubicación del móvil.

Una vez armados y descifrados los datos suministrados por el móvil, se tienen los siguientes parámetros que serán utilizados para el cálculo de ubicación:

(a) Identificador de la celda que da cobertura al móvil (Cell ID)
(b) Nivel de potencia recibido de la celda servidora (RXLEV-FULL-SERVING- CELL)
(c) Número de celdas servidoras que está monitoreando el móvil (NO-NCELL)
(d) Nivel de potencia recibido por las celdas vecinas (RXLEV-NCELL)
(e) Índice de la lista de vecinas correspondiente al BCCH (BCCH-FREQ-NCELL)
(f) Lista que contiene el canal de RF asignado a cada celda vecina (BCCH channel list)

(g) Código de identificación de la celdas servidoras (BSIC-NCELL)

4.3.2. Método de comparación directo celda a señal

El método principalmente se apoya en datos de la huella de cobertura que son obtenidos para el estudio y optimización de la red llamada “Drive Test”. El drive test contiene información concerniente a niveles de potencia de las estaciones, identificación de las celdas (Cell ID), BCCH, BSIC y altura sobre el nivel del mar, todo referido a una posición geográfica. Éste consiste en el registro de datos obtenidos de la red por medio de un equipo de medición especial que realiza un barrido en frecuencia para obtener la información pertinente a un conjunto de portadoras de RF que se están monitoreando en ese preciso instante. Este equipo toma como referencia las coordenadas geográficas del punto donde se captura la medición y a partir de ésta vacía los datos obtenidos, resultando así un archivo que contiene parámetros de la red para posiciones geográficas especificas. Luego este archivo es procesado y filtrado para obtener otro archivo llamado “grilla”, que contiene información de la red por sectores o rejillas. Esto no es más que subdividir una zona en sectores más pequeños, que encierran el número de estaciones que llegan a él, obteniendo así el número de estaciones que llegan a ese sector y la información asociada a estas. Esto se podría ver como una gran zona geográfica dividida en muchos subrectángulos como si fuese una rejilla. Cada rejilla contiene un conjunto de información asociada a la red y determina el conjunto de estaciones que dan cobertura a esa área específica.

Cabe destacar que estas mediciones son realizadas en vehículos a una velocidad no mayor de 60 Km/h, velocidad a la cual puede responder adecuadamente el GPS para evitar errores de lectura. También hay que tomar en cuenta que estas mediciones son tomadas en vías y calles donde pueden pasar autos, en pocas palabras el drive test se realiza a nivel de arterias viales. En la siguiente figura se observa el esquema general de la grilla.

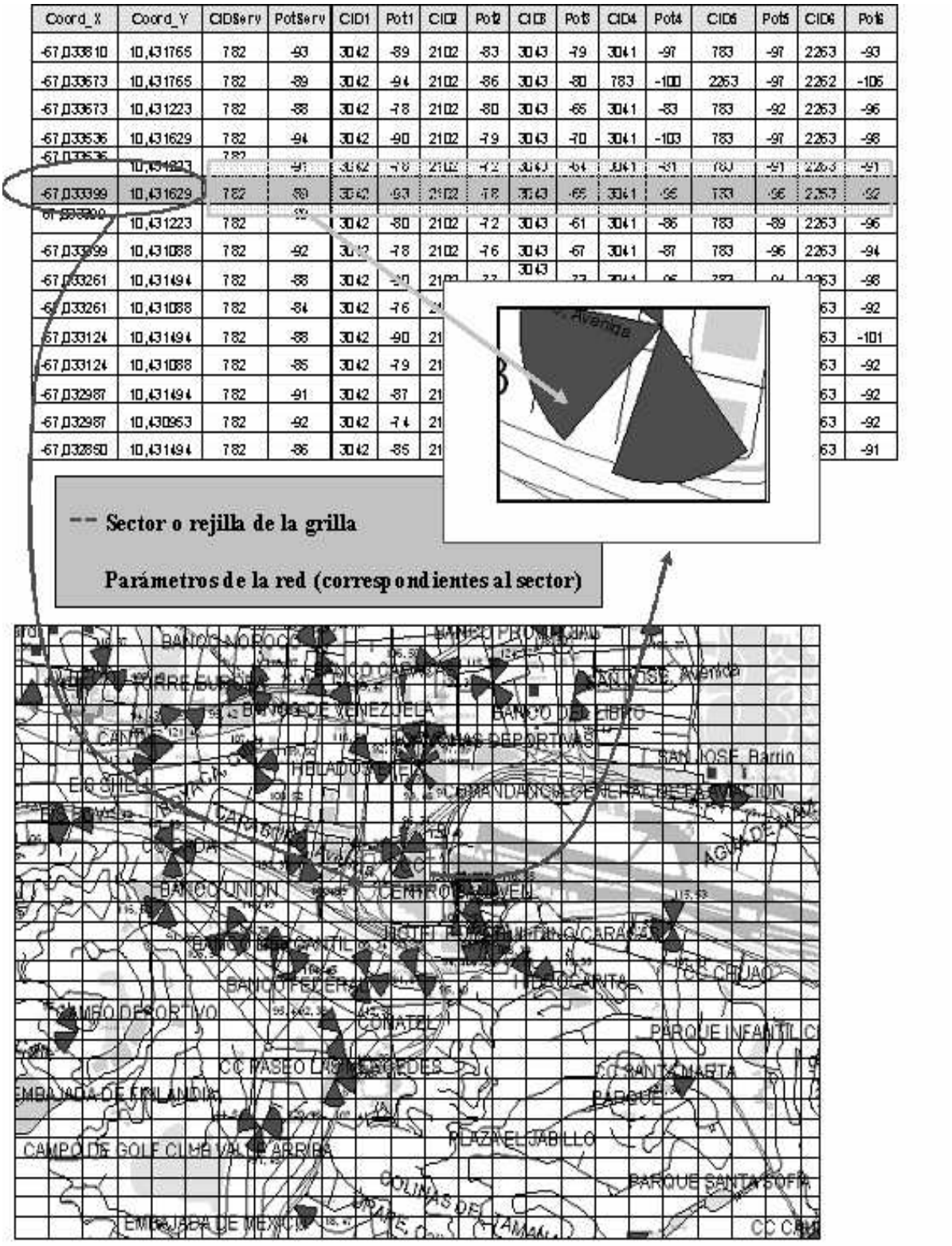

Figura 4.5. Esquema general de la grilla

Para diseñar el método más apropiado para estimar la ubicación del móvil se comenzó con la recolección de muestras de los parámetros obtenidos por este en zonas donde se conocía su posición. Esto consistió en tomar la referencia geográfica del lugar (coordenadas geográficas) con la ayuda de un GPS marca GARMIN cuyas características técnicas son similares a los usados para los drive test, y a la vez solicitar la información de la red para ese punto particular. Esto se repitió para diferentes puntos de interés con la finalidad de obtener una muestra representativa de los diferentes escenarios que se pueden presentar a la hora de intentar obtener la posición de un móvil.

.

Una vez obtenida esta información se comenzó por relacionarla con los datos arrojados por el drive test. Para esto ubicamos los datos suministrados por el drive test para el mismo punto de prueba y una vez ubicado se comenzó por analizar si la información de la red obtenida correspondía o se asemejaba a la suministrada por el móvil, obteniendo los siguientes detalles:

- La información suministrada por el drive test no especifica directamente cual es la estación servidora, sólo da un conjunto de estaciones con sus respectivos niveles de potencia para una rejilla en particular.
- En los datos arrojados por el drive test se observa que existen estaciones que poseen niveles de potencia por encima de los -48 dBm.
- Para una rejilla en particular del drive test pueden existir más de 6 estaciones que den cobertura al móvil.
- Los datos contenidos en una rejilla no están ordenados, es decir; pueden existir casos donde el primer valor de potencia de la rejilla correspondiente a una estación sea el menor de todos o que sea el mayor. En la mayoría de los casos la información no guarda relación alguna.
- La información original del drive test contiene el parámetro altura sobre el nivel del mar, el cual es innecesario para el cálculo de la ubicación.
- El drive test solo es válido a nivel de calles, autopistas y avenidas.
- Los niveles de potencia suministrado por el móvil son truncados si los niveles recibidos por él están por encima de los -48 dBm. Si los niveles recibidos está por encima al antes expuesto, el móvil los devuelve fijándolos a -48 dBm.
- Los niveles de potencia recibidos van a depender del equipo utilizado, aunque la diferencia es de unos cuantos dBm.
- Los niveles de potencia varían al tomar diferentes muestras para un mismo punto de referencia.

Partiendo del planteamiento anterior se tomaron una serie de acciones a fin de poder acondicionar los datos del drive test de manera que correspondiese y se asemejara más a los datos enviados por el móvil. Las acciones tomadas fueron las siguientes:

- Se eliminó la información innecesaria para el cálculo de ubicación, información que sólo hace que el archivo sea más pesado y que la búsqueda dentro del mismo sea más lenta.
- Se le dio un procesamiento especial a los datos de Cell Id – Potencia. Esto se hizo ordenando los registros por niveles de potencia, es decir; de manera decreciente. Se ordenaron los pares Cell Id – Potencia de manera que siempre el primer par fuese el de mayor potencia.
- Una vez ordenados los datos del drive test se asumió que el primer Cell Id de cada registro o rejilla, es el correspondiente al de la estación servidora.
- En casos donde existía el mismo nivel de potencia pero Cell Id diferentes y estos niveles de potencia a su vez eran los máximos para el registro o lo que es lo mismo decir que se tenían dos posibles estaciones servidoras; se optó por insertar otro registro repitiendo la misma información pero colocando en ambos servidoras distintas. Esto se hizo para las distintas combinaciones que pudiesen existir, 2, 3, 4 y hasta 5 posibles estaciones con niveles de potencia iguales pero con Cell Id diferentes.
- Otra de las depuraciones realizadas fue el filtrar la información de cada registro tomando en consideración que para cada rejilla sólo debe existir una posible estación servidora y las posibles estaciones vecinas definidas por el estándar y que pueden ser máximo 32. Tomando en cuenta que el equipo de medición lo que realiza es un barrido en frecuencia para un grupo de portadoras predeterminadas, existe la posibilidad de capturar información de estaciones muy alejadas al lugar donde se efectuaron las mediciones cuyos niveles de recepción son muy bajos además de no estar definida como posible vecina de la estación servidora. Para realizar la depuración se buscó la estación servidora correspondiente a cada rejilla y se cotejó contra una base de datos que poseía la información de las posibles celdas vecinas definidas para cada estación. Una vez que se conoce el conjunto de estaciones vecinas por estación servidora, se procedió a eliminar la información de las estaciones vecinas contenidas en cada registro no pertenecientes al conjunto.
- Se sabe que un registro del drive test el cual corresponde a una rejilla puede contener la información de más de 7 estaciones. Tomando en cuenta que la primera es la estación servidora y las restantes son las vecinas, se eliminó la información adicional; es decir se fijó el archivo a que solo tuviese información de la estación servidora y de las 6 correspondientes estaciones vecinas, resultando así un archivo menos pesado y más depurado.

Uno de los detalles importantes son los constantes cambios que se presentan en los niveles de recepción cuando el móvil monitorea los niveles de potencia de las estaciones que le dan cobertura. Para estimar qué tanto pueden variar los niveles de recepción del móvil se tomaron un conjunto de mediciones en ambientes abiertos para un mismo punto de referencia, resultando para el momento que la potencia podía variar hasta 5 dBm alrededor de la media. Tomando en cuenta esto y el truncamiento de los niveles de recepción se diseñó un método que fuese capaz de obtener la ubicación del móvil.

4.3.3. Descripción del método propuesto

El método de localización propuesto es el siguiente:

(a) Obtenido el Cell Id de la estación servidora hacemos el primer filtraje en los datos previamente depurados del drive test. Esto consiste en obtener sólo los registros para los cuales la estación servidora corresponda a la obtenida por el móvil. Realizado esto tenemos el primer conjunto de registros que contendrán las primeras estimaciones de ubicación.

(b) Una vez obtenido el conjunto de posibles estaciones servidoras realizamos un segundo filtraje con el nivel de potencia de la servidora. Para esto se debe tener en cuenta la siguientes premisas:

- Si el nivel de recepción es menor o igual a -48 dBm realizar un segundo filtraje aplicando la siguiente ecuación:

$$2\ dBm + RXLEV \leq RXLEV \leq RXLEV - 2\ dBm \quad \textit{Ecuación 4.1}$$

  Esto no es más que capturar todos los registros cuyo nivel de recepción se encuentren por encima o por debajo en 2 dBm o lo que es lo mismo capturar todos los registros que se encuentren en este intervalo. RXLEV es la potencia recibida por el móvil.
- Si el nivel de potencia es superior a los -48 dBm realizar el filtraje aplicando la siguiente ecuación:

$$RXLEV > -48\ dBm \quad \textit{Ecuación 4.2}$$

  Esto se hace debido a la limitación en los niveles de recepción que se obtienen en la información que es tomada del teléfono. Con la ecuación 4.2 se evalúan todos los casos posibles en cuanto a los niveles de potencia que se podrían haber monitoreado en ese instante. Aunque hay

que tomar en cuenta que en la mayoría de los casos este nivel siempre se encuentra por encima de los -48 dBm.

(c) Con los registros obtenidos una vez aplicados los pasos anteriores, se realizan una serie de filtros que consisten en:

- Aplicar el procedimiento descrito en b (discriminación de registros mediante las ecuaciones 4.1 y 4.2) pero esta vez tomando en cuenta la potencia de la primera celda vecina para el filtraje. Esto arroja como resultado otro conjunto de registros con las posibles estimaciones de ubicación.
- Aplicado el filtro anterior se realiza otro filtro pero esta vez aplicado con el nivel de potencia de la segunda mejor celda vecina. Esto vuelve arrojar otro conjunto de posibles registros de ubicación.
- Una vez aplicada el segundo filtro se procede en realizar el tercero y último filtro, aplicado a los registros resultantes de los dos primeros filtrajes, para así obtener una serie de registros preliminares con los posibles puntos de ubicación.

(d) Una vez obtenido el conjunto de registros que contienen las posibles posiciones de donde se podría encontrar el móvil, se calculó el promedio de las coordenadas geográficas dadas por éstos. Este promedio contiene la ubicación estimada a través del método de ubicación propuesto.

Una vez diseñado el método que obtendrá la ubicación del móvil se procedieron con las pruebas para verificar su comportamiento en los diferentes escenarios posibles. Estas pruebas se realizaron en la ciudad de Caracas y se verán con detalle en el siguiente capítulo.

4.4. Descripción del programa desarrollado para estimar la ubicación del móvil

El programa en primera instancia está atento a las solicitudes de ubicación enviada por el ESME, el cual le envía los datos de solicitud de ubicación. Una vez recibida la solicitud de información se encarga de decodificar los datos enviados y estructurarlos para su procesamiento. En la decodificación se obtienen los siguientes parámetros:

- Cell ID (Identificador de la estación servidora)
- RXLEV-FULL-SERVING CELL (Nivel de potencia correspondiente a la estación que da cobertura al móvil)

- NO-NCELL (Número de estaciones vecinas monitoreadas por el móvil)
- RXLEV-NCELL (Nivel de potencia correspondiente a la estaciones vecinas)
- BCCH-FREQ-NCELL (Índice de la lista correspondiente al BCCH)
- BSIC-NCELL (Código de identificación de las estaciones vecinas)
- BCCH channel list (Lista de BCCH)
- Header (Identificador del tipo de servicio demandado)

Estos son los parámetros que se utilizarán para estimar los cálculos de ubicación. El programa hará conexiones a base de datos remotas. Estas bases de datos se diseñaron en MySQL, un servidor de base de datos bastante rápido y el cual es software libre. Ésta contendrá información de todas las estaciones de la red de Digitel, contendrá la información del drive test e información de los servicios demandados; es decir tablas que contienen información de servicios básicos con su respectiva ubicación en coordenadas geográficas. El servidor de base de datos puede estar en el mismo servidor donde se encuentra la aplicación tipo ESME que recibe las solicitudes de ubicación que luego les son enviadas a la aplicación para el procesamiento de ubicación, o en un servidor independiente.

El programa realizado recibe la solicitud de ubicación en primera instancia, luego descifra y desglosa los datos recibidos en los parámetros antes expuestos. Primero verifica qué tipo de servicio le han solicitado y lo guarda para su futura búsqueda en la base de datos de servicios. Con el dato del Cell ID se realiza una conexión a la base de datos y se extraen todos los datos que correspondan a esta estación. Estos datos servirán para realizar el filtraje en los datos del drive test.

Como se sabe el BCCH-FREQ-NCELL arroja el índice en que se encuentra el valor del BCCH de las estaciones vecinas monitoreadas por el móvil. Realizando una consulta a la información del BCCH channel list la cual es ordenada e insertada en un arreglo, se puede obtener el valor del BCCH, comparando el índice del BCCH-FREQ-NCELL con el índice del arreglo donde se encuentra el BCCH channel list, esto dará como resultado la identificación del BCCH correspondiente. Una vez obtenido este valor el programa compara la dupla BCCH-BSIC contra la tabla que contiene la información de las posibles

estaciones vecinas para el Cell ID de la estación servidora y encuentra los valores del conjunto de Cell ID de las celdas vecinas. Una vez hecho esto se tiene los Cell ID de todas las celdas vecinas dadas por el móvil y que pueden ser máximo 6.

Conociendo las posibles celdas definidas para la estación servidora se realiza una consulta a la tabla de la base de datos que contiene la información del drive test. Una vez conectados a esta tabla la primera consulta de selección que se realiza es filtrar por Cell ID, luego se aplican los criterios de filtraje antes descritos hasta obtener la estimación de la ubicación del móvil.

Con la información que resulta del filtraje del drive test que no es más que la obtención de las coordenadas x, y de la posición geográfica, se realiza una consulta a la tabla de la base de datos que contiene los servicios, esto tomando en cuenta el identificador de servicio capturado. Una vez conocido el identificador sabemos a qué tabla de servicios específica consultar y de esta manera se podrán obtener la información concerniente para ser devuelta al móvil que originó la solicitud.

En las siguientes figuras se observa el diagrama de flujo correspondiente al programa desarrollado.

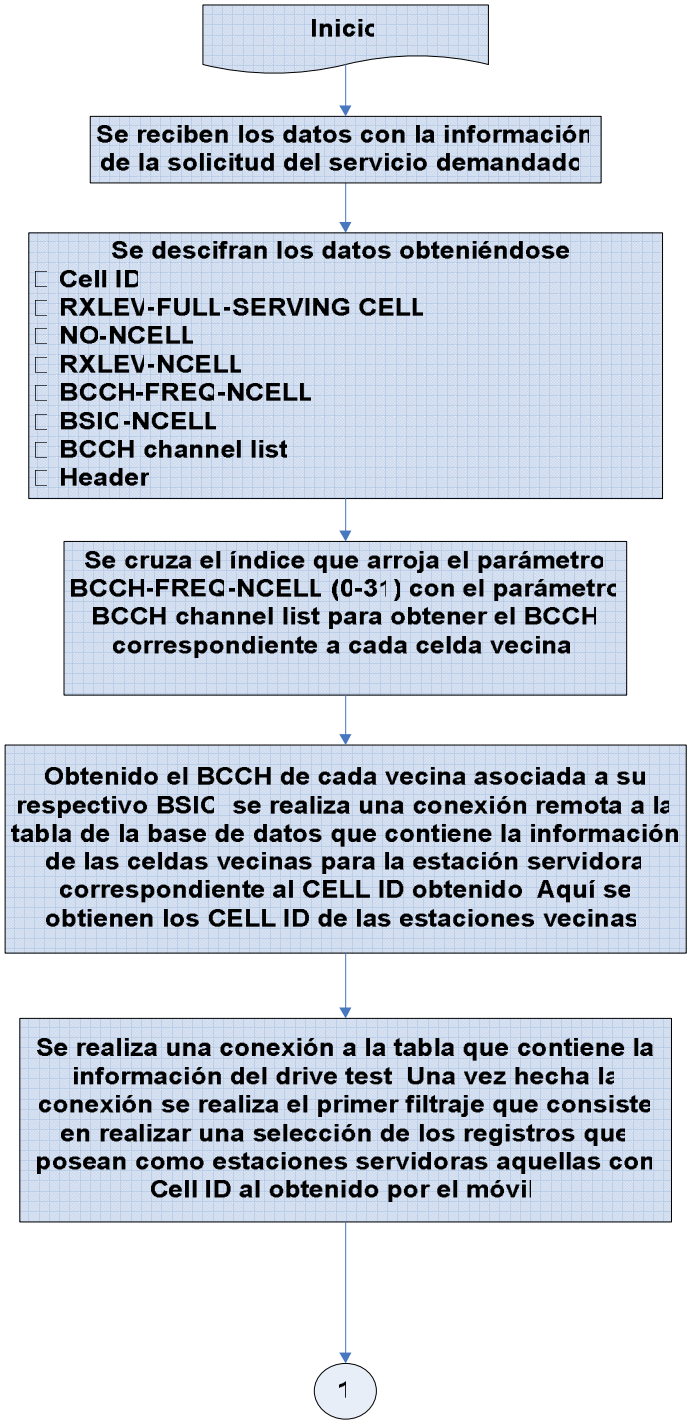

Figura 4.6. Diagrama de flujo del programa para el cálculo de ubicación.

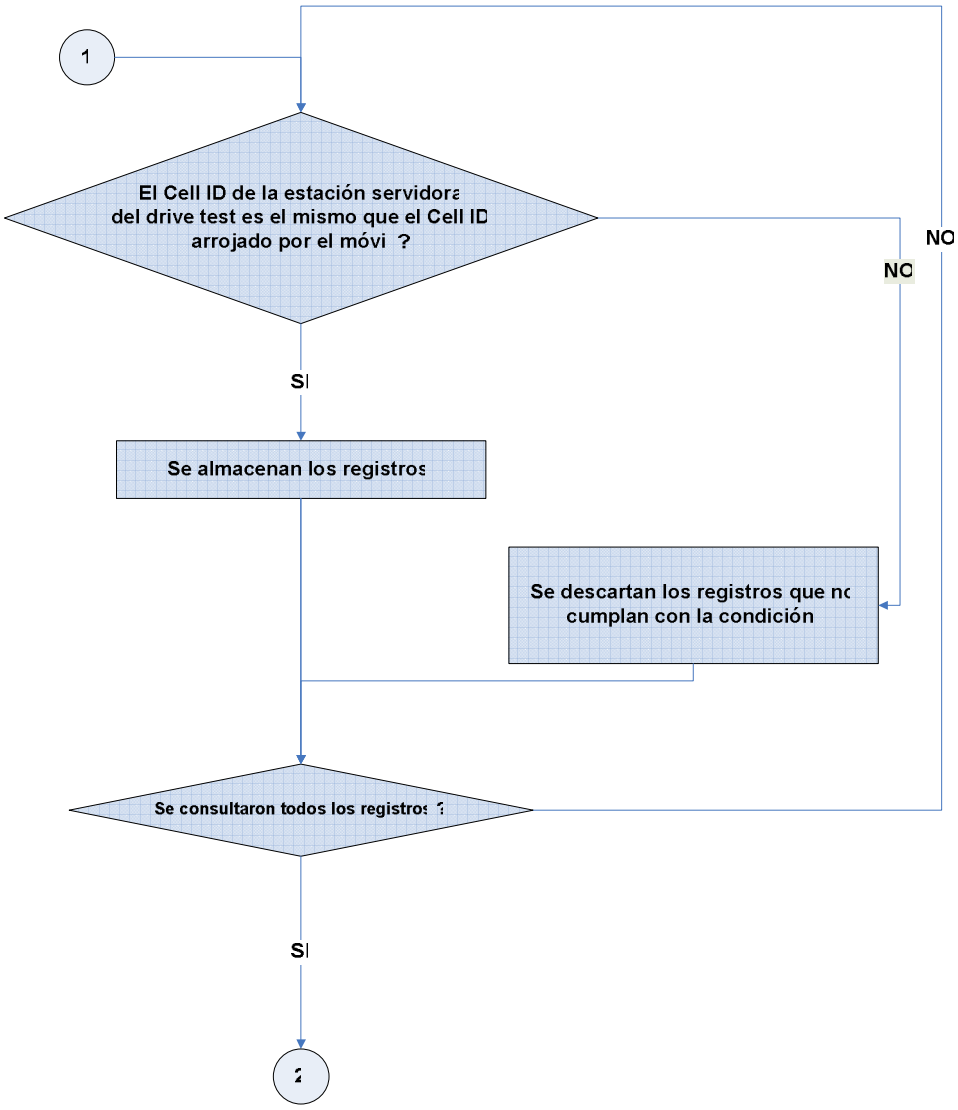

Figura 4.7. Diagrama de flujo (continuación)

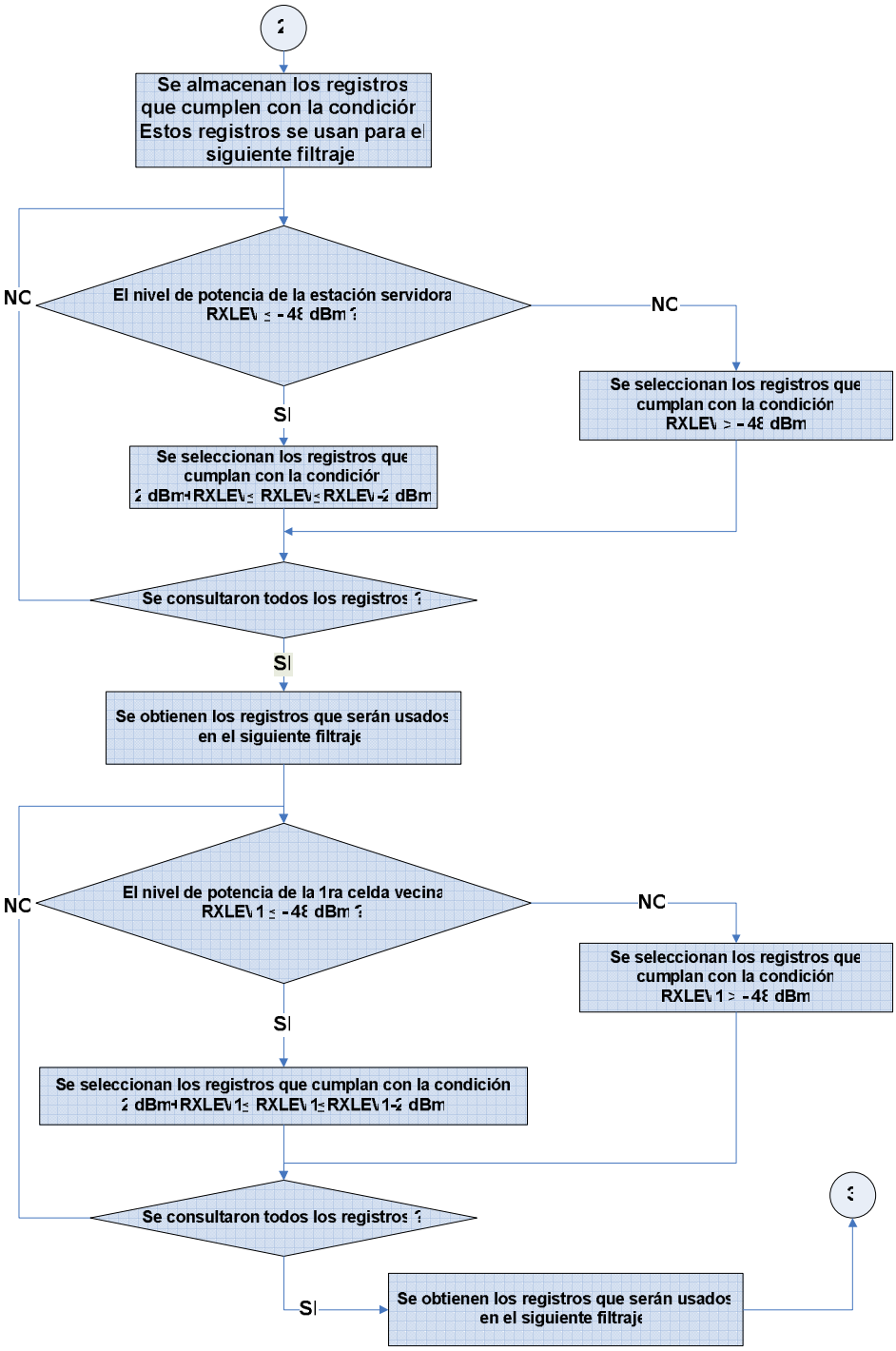

Figura 4.8. Diagrama de flujo (continuación)

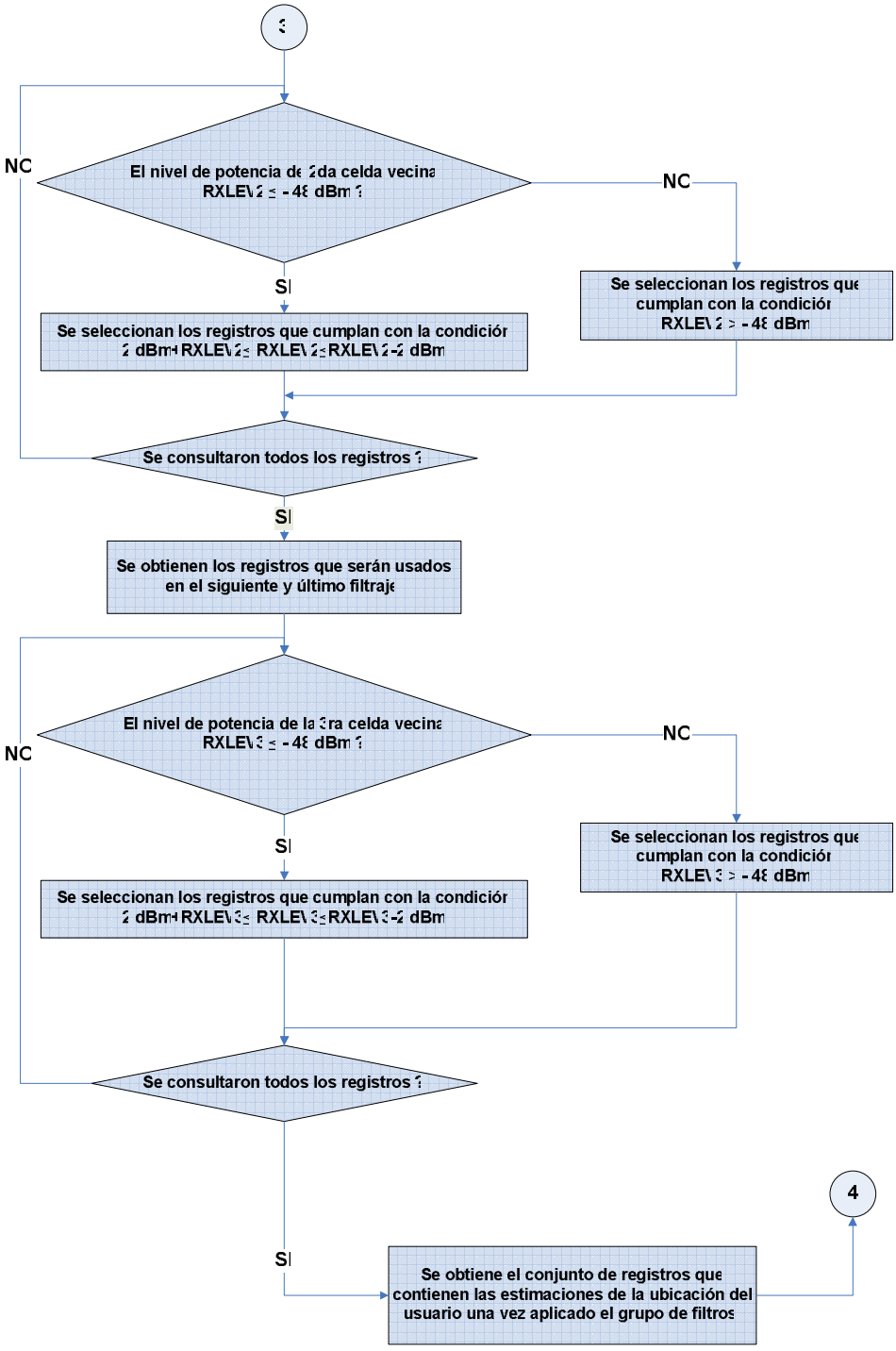

Figura 4.9. Diagrama de flujo (continuación)

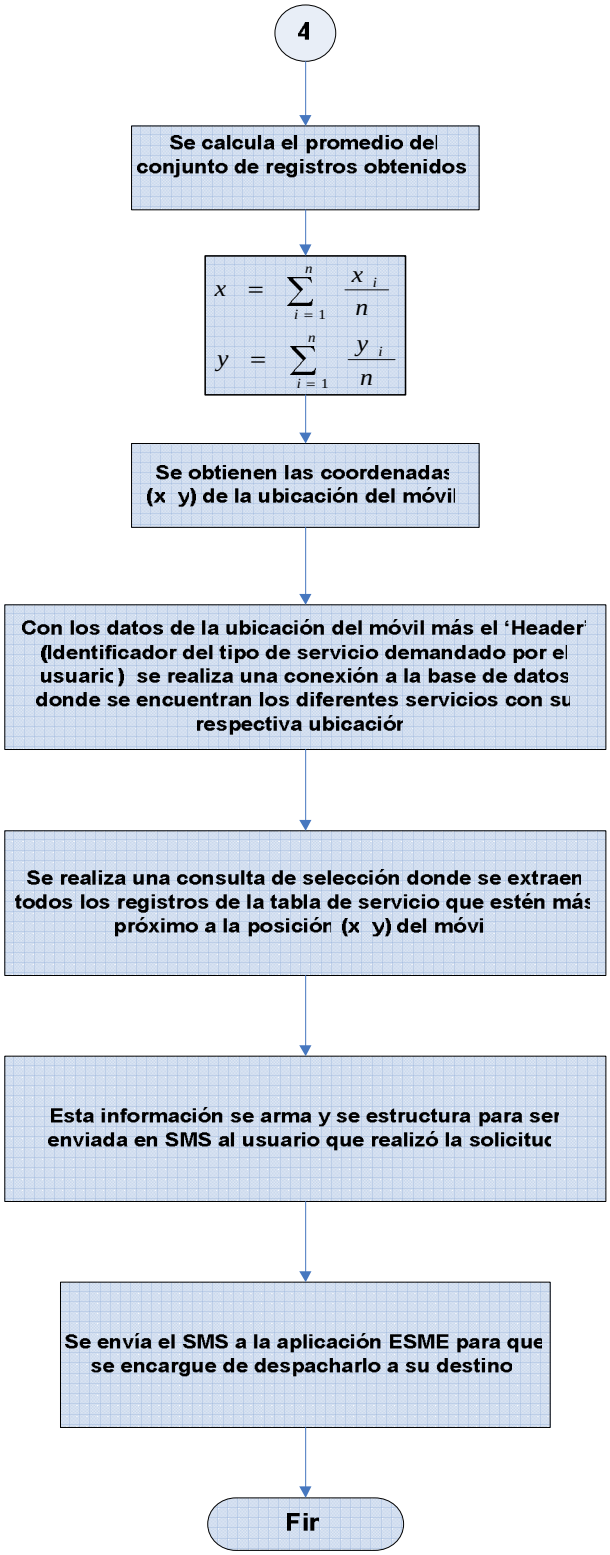

Figura 4.10. Diagrama de flujo (continuación)

CAPÍTULO V

ANÁLISIS DE RESULTADOS

5.1. Resultados de las pruebas realizadas en la ciudad de Caracas

Para la comprobación del método propuesto se realizaron una serie de pruebas en la ciudad de Caracas con la finalidad de calcular el error cometido al tratar de estimar la posición del usuario que realiza la solicitud.

Los equipos empleados para llevar a cabo estas pruebas fueron un GPS marca GARMIN y un teléfono celular NOKIA 7200. El GPS posee características similares a los que se usan para el drive test. El teléfono NOKIA es de los que poseen antena integrada al chasis.

Para las pruebas se programó la aplicación para que recibiera la información de localización, la procesara y estimara su posición, para que luego fuese guardada en una base de datos que serviría para cotejar contra las estimaciones obtenidas por el GPS. El procedimiento para capturar los datos consistió en enviar solicitudes de ubicación al servidor de localización para que este estimara la posición, luego de enviada la solicitud se capturaron las coordenadas (x, y) del lugar donde se realizó la solicitud con la ayuda del GPS. Al capturar la información mediante el GPS se tuvo el cuidado de tomar las mediciones lo más puras posibles, es decir; se cuidó que para tomar una lectura como válida el GPS estuviese estabilizado y recibiendo al menos la señal de cuatro satélites, con niveles de potencia óptimos. Se colocó el GPS en un modo en el que muestrea las coordenadas de la posición a un intervalo regular para luego sacar el promedio de las posiciones calculadas; de esta manera la medición es más fiable. Otro aspecto que se cuidó es que existiera la línea de vista al espacio, dicho de otra manera no estar debajo de arbustos, al lado de edificios de gran tamaño u cualquier otro obstáculo que pudiese interferir en la obtención de la medición.

Este proceso se repitió consecutivamente hasta obtener una muestra representativa de 176 puntos. Una vez que se obtuvieron los datos arrojados por el servidor de localización al igual que los obtenidos a través del GPS, se procedió a calcular el error cometido al utilizar el método de localización propuesto.

Los resultados de las pruebas al calcular el error cometido se muestran a continuación:

Algunos datos relevantes son:		
Media:	**148,72 m**	
Desviación Estándar:	**120,85 m**	
Máximo:	**972,27 m**	
Mínimo:	**4,89 m**	
% de medidas entre 0 y 50 metros		**11,66%**
% de medidas entre 50 y 100 metros		**30,06%**
% de medidas entre 100 y 150 metros		**20,86%**
% de medidas entre 150 y 200 metros		**15,95%**
% de medidas entre 200 y 250 metros		**7,97%**
% de medidas entre 250 y 300 metros		**6,13%**
% de medidas entre 300 y 350 metros		**1,84%**
% de medidas entre 350 y 400 metros		**1,84%**
% de medidas entre 400 y 450 metros		**1,84%**
% de medidas entre 450 y 500 metros		**0,61%**

Tabla 5.1. Datos del error cometido

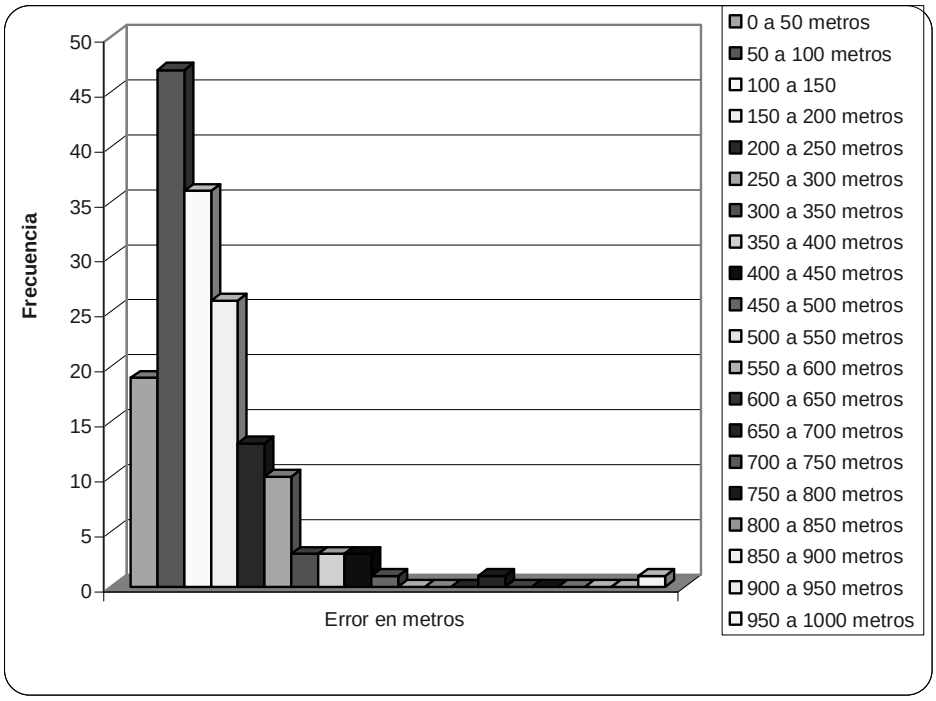

Figura 5.1. Gráfica del error cometido

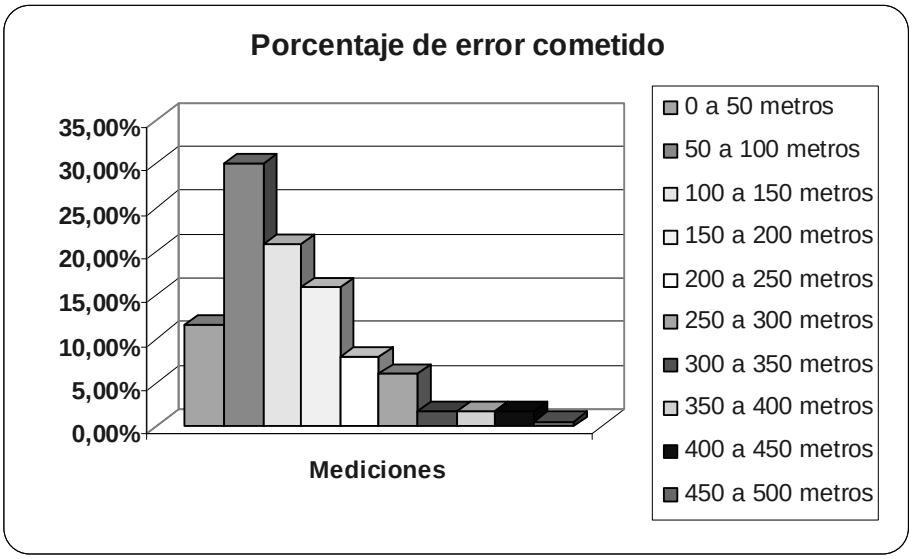

Figura 5.2. Porcentaje de error cometido

Realizando el análisis de los datos obtenidos se tiene que para el universo de 176 muestras a las cuales les fue aplicado el método de localización, a 163 se le

encontró solución; es decir que el método no encontró las coordenadas de la posición del móvil para las demás. Esto equivale al 92,61% de las muestras, y se puede decir el método es fiable debido a que tiene la precisión de hallar una solución de localización en el 90% de los casos (sin hablar de precisión). El otro 10% a los que no se les encuentra solución se le puede dar un procesamiento alterno a fin de garantizar una solución viable a cada solicitud de ubicación.

Una posible alternativa para ese 7,39% de las muestras a las cuales no se le encontró solución por el método propuesto, es la de asignar la posición de la coordenada (x,y) de la radio base que le da cobertura en ese instante al móvil; es decir, suponer que el usuario tiene coordenadas idénticas a las de la estación servidora.

De la tabla 5.1 se tiene que el error cometido promedio del método es de 148,72 metros, con una desviación estándar de 120,85 metros. Esto quiere decir que la precisión puede estar acotada en el intervalo de 148 ± 120 metros, es decir; entre 28 metros y 268 metros aproximadamente. El hecho de que la desviación estándar sea alta es una medida de que los datos no están concentrados sino dispersos, y que se pueden encontrar en el rango antes descrito. Los valores del máximo y el mínimo error cometido son de 972,27 metros y 4,89 metros respectivamente. Estos valores son muy tolerables respecto a métodos más elaborados y que involucran elementos adicionales para su desarrollo.

En la figura 5.1 se observa cómo la mayoría de los errores cometidos se sitúan por debajo de los 200 metros, es decir, existen mayores concentraciones de solicitud de ubicación con errores inferior a los 200 metros. Si se observa la figura 5.2, la cual da el detalle del porcentaje de error cometido, se tiene que existe un mayor porcentaje de solicitudes cuyo error se encuentra entre los 50 y 100 metros; el cual representa el 30,06% de la población. Luego le sigue un porcentaje de la población con error comprendido entre los 100 y 150 metros, que viene a representar el 20,86% de las muestras. Por último le sigue una muestra

significativa que representa el 15,95% de las muestras y se encuentra entre los 150 y 200 metros de error cometido.

De lo antes mencionado y al ver con detenimiento la tabla 5.1 y la figura 5.2 se puede decir que el 78,53% de las muestras presentan un error menor a los 200 metros y el 62,57%, un error menor a los 150 metros. En otras palabras el error cometido al aplicar el método de localización en la mayoría de las muestras ronda los 200 metros.

En la figura 5.3 se observa el error cometido al estimar la posición del usuario asumiendo las coordenadas de la estación que le da cobertura. Esta muestra es la del conjunto de solicitudes a las cuales no se les encontró solución con el método propuesto.

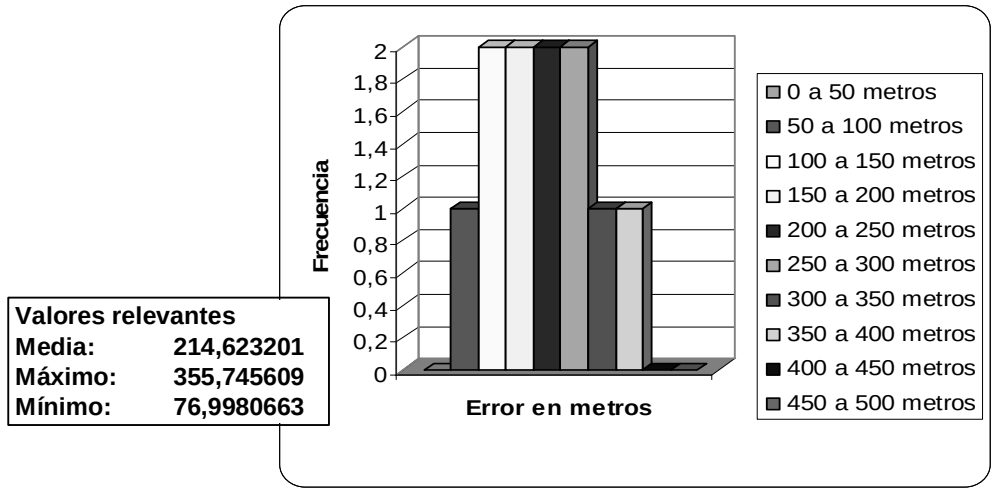

Figura 5.3. Error cometido a nivel de Cell ID cuando el método no arroja resultados.

En la gráfica 5.3 se muestra el error que se comete al tratar de estimar la ubicación del usuario a nivel de Cell ID. Como se observa el error se encuentra alrededor de los 200 metros en zonas donde la cobertura de las celdas no es muy amplia. Para ubicar un usuario en una zona urbana donde el rango de cobertura de las celdas no es muy amplio es factible ubicarlo sólo a nivel de Cell ID, debido a que ofrece precisiones aceptables en entornos urbanos.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

Actualmente existen en el mercado diversos métodos y sistemas para el desarrollo de plataformas capaces de ofrecer servicios basados en localización LBS (Location Based Services), tanto es así que tenemos métodos capaces de ubicar a un móvil conociendo la identidad de la celda que le da cobertura, métodos basados en la red, métodos basados en modificación del móvil y los llamados métodos híbridos que vienen siendo una combinación de los antes mencionados. El método a implementar dependerá de los operadores de la red que para esto deberán tomar en cuenta el impacto económico capaz de soportar, el tiempo de implementación y la manera más fácil de ofrecerlo a los usuarios.

Los métodos basados en Cell ID son los menos onerosos y a su vez los más fáciles de implementar, debido a que no se necesitan realizar cambios a nivel de la red, no necesitan de grandes inversiones para su desarrollo y son rápidos y fáciles de implementar; lo cual no ocurre con los métodos basados en la red, en el móvil y algunos métodos híbridos.

El método presentado en el desarrollo de este documento propone la implementación de un sistema con capacidad de tomar parámetros de la red mediante una sencilla aplicación en la SIM que es capaz de realizar los procedimientos necesarios para que el teléfono solicite información a la red y la devuelva a ésta, para que luego pueda ser enviada a un servidor encargado del procesamiento y cálculo de ubicación. Desde el punto de vista de equipos necesarios para implementarlo, sólo se necesita programar una SIM, tener una PC que tenga las prestaciones de servidor y un teléfono. A nivel económico el impacto es mínimo, tanto para el usuario como para el operador de la red. A nivel de red, no existen modificaciones, el operador sólo necesita disponer de un servidor y listo. A nivel de usuario el impacto radica en la adquisición o

adecuación de la tarjeta SIM; esta puede ser reprogramada o sustituida por completo.

Si analizamos un poco lo antes mencionado nos damos cuenta que el despliegue de una plataforma de localización con estas características es muy factible y atractivo para operadores que quieran dar sus primeros pasos en ofrecer servicios basados en localización. Si se quiere la implementación de este tipo de desarrollos es la evolución natural de dichos servicios, debido a que sirve como referencia para estudiar el comportamiento y la aceptación por parte del público, frente a este tipo de aplicaciones. Esto les permitirá evaluar y si es necesario realizar los cambios pertinentes a fin de ofrecer un servicio acorde a las solicitudes y exigencias de los usuarios.

De los resultados obtenidos en las pruebas realizadas se demuestra que el método de localización presenta un error aceptable que se encuentra entre los 28 y 268 metros aproximadamente, error admisible al compararlo con otras técnicas y plataformas existentes como la de Movistar con su servicio Localízame, el cual consiste en un servicio de localización al que los usuarios solicitan información de ubicación de otros usuarios y se les responde con la información de la localización que viene dada en un SMS o locución, que indica la posición aproximada en un margen de error de 200 metros en ciudad y de 5 a 20 kilómetros en zonas rurales.

Para el despliegue de una plataforma como la descrita en el documento, se tendría que contar con la información del drive test de toda la zona de cobertura de la red de Digitel. Partiendo de ese punto de vista esta es una de las limitantes más fuertes, debido a las siguientes premisas:

- El drive test sólo es válido a nivel de calles, carreteras y avenidas; es decir sólo es válido a nivel de arterias viales.
- Actualmente no existe drive test para toda la zona de cobertura de la red de Digitel. Las zonas que actualmente tienen drive test son: Caracas, Maracay, Valencia y unas que otras zonas de importancia.
- Los drive test son realizados anualmente o semestralmente, tiempo en el cual la información puede estar desactualizada.

- Es necesario realizar drive test cada vez que entre en servicio una nueva estación de la red, o al menos es necesario realizarlo en la zona de acción de la nueva estación. Una vez hecho esto se debe actualizar la base de datos que contiene la información concerniente a el.
- Los costos para la realización de drive test son elevados, y si se toma en cuenta que se necesitan realizar periódicamente, esto hace que no sea viable el desarrollo de la plataforma de localización mediante esta vía.
- Los drive test deben ser bien cocidos, es decir; se necesita recorrer la mayor cantidad de área posible, para así obtener una información más fidedigna.
- El realizar un buen drive test lleva su tiempo, esto quiere decir que si ocurren cambios en la red y se quiere volver a capturar esta información para mantenerla actualizada; se deberá esperar lapsos de 1 mes y hasta más dependiendo de la zona a recorrer.

Otras de las limitantes para el desarrollo de esta plataforma es la capacidad de almacenamiento de la SIM, ya que se sabe que es de espacio restringido en memoria. El programa desarrollado ocupa muy poco espacio en la SIM, pero hay que tomar en cuenta que el menú implementado en él es pequeño y pensando en el futuro crecimiento de la aplicación se podría requerir de una mayor capacidad para albergar menús de gran envergadura. En el desarrollo de la aplicación se utilizaron tarjetas SIM de 32K de memoria, aunque actualmente Digitel ofrece SIM de 64K y en el mercado ya existen las de 128K y versiones superiores. Disponiendo de SIM con prestaciones como éstas ya la limitante no estaría aquí, sino en la capacidad del usuario de adquirirla.

Otro de los temas importantes a la hora de desplegar una plataforma de este tipo está en las base de datos de servicios. Estas bases de datos son especializadas ya que deben contener las coordenadas geográficas del servicio solicitado. Los proveedores de bases de datos generalmente no tienen estas bases de datos completas, sólo las tienen para algunas categorías y las otras poseen la ubicación pero a nivel de direcciones. También vale destacar lo caro que resulta el obtener esta base de datos con dicha información. Para el desarrollo de la plataforma de prueba se usaron bases de datos que fueron estructuradas y armadas manualmente.

Se pudieron armar un total de 9 diferentes tablas de servicios como:

(a) Bancos

(b) Hoteles

(c) Farmacias

(d) Estaciones de servicio

(e) Restaurantes

- Españoles
- Italianos
- Areperas
- Chinos

(f) Sitios turísticos

Estas tablas de servicios son las que se usan para la plataforma de pruebas montada actualmente. Cabe destacar que las tablas no están muy completas debido a como se mencionó fueron armadas manualmente y no están bien dotadas de información.

Este tipo de servicios de localización no está regulado en Venezuela por ningún ente regulador (Conatel), es el operador de la red que debe garantizar y dar la seguridad de no revelar la posición del usuario para otros fines ajenos a los suyos. El tipo de servicio ofrecido es del tipo no intrusivo, es decir; que no se realizan cálculos de ubicación del usuario sin que éste los haya solicitado. De esta manera se puede decir que la localización de usuarios con este servicio es unidireccional, además de saber que la SIM no puede realizar peticiones de localización sin que se le indique.

Para finalizar vale acotar que este es un desarrollo nacional que está a la par de productos similares que se encuentran en el mercado y cuyos precios de implementación son muy elevados. A nivel de costos a la hora de implementar el servicio, se puede decir que los mismos son muy bajos y bastantes competitivos con los precios del mercado hoy en día.

REFERENCIAS BIBLIOGRÁFICAS

[1] García, Andrés; Sáez María. Telefonía Móvil. Escuela Politécnica Superior de Albacete de la Universidad de Castilla-La Mancha. Dirección electrónica: http://www.info-ab.uclm.es/labelec/Solar/Comunicacion/Telefonia_movil/index_archivos/Page1167.htm. [Consulta: 2005]

[2] SMPP Forum. Short Message Peer to Peer Protocol Specification (v3.4. del 12 de Octubre de 1999, Issue 1.2).

[3] ETSI TS 101 267 V8.16.0 (2004-03). (GSM 11.14 version 8.16.0 Release 1999)

[4] ETSI TS 100 557 V4.24.0 (2002-12). (GSM 04.08 version 4.24.0 GSM Phase 2)

[5] Hernández, Daniel. Propuesta de plataforma y método de ubicación de usuarios en una red GSM, a partir de la medición de la intensidad de la señal, (Tesis)—Caracas: Universidad Central de Venezuela, 2005.

[6] Bernardos, Ana, Carlos III, U. Tecnologías de localización. Centro de Difusión de Tecnologías ETSIT-UPM. Diciembre, 2003. Dirección electrónica: http://www.ceditec.etsit.upm.es/localizacion.php.

[7] Flores, Joel A. Desarrollo e implementación de un sistema de mensajería corta (SMS) para la Universidad Central de Venezuela, (Tesis)--Caracas: Universidad Central de Venezuela, 2004, p.21.

ANEXOS

ANEXO 1. DESCRIPCIÓN DEL PROGRAMA RESIDENTE EN LA TARJETA SIM

Filosofía de la aplicación a desarrollar en la tarjeta SIM

En este punto se describirá la filosofía de la aplicación a desarrollar a nivel de SIM para obtener los parámetros necesarios que nos permitan estimar la posición del usuario que realice la petición de ubicación. Es lógico que para estimar la posición de un móvil hacen falta conocer ciertos datos del mismo y de la red. En nuestro caso estos serán proporcionados por el teléfono a la tarjeta SIM, mediante comandos que se le envían a través de una aplicación que reside en la tarjeta y que le indica que parámetros obtener de la red. Estos comandos serán descritos mas adelante y forman parte de un estándar especificado por la ETSI (*European Telecommunications Institute*), el cual define la interfaz para la interacción entre el teléfono y la SIM.

La filosofía de la aplicación a desarrollar en la SIM, es diseñar un programa que sea capaz de desplegar un menú de opciones donde el usuario elija el tipo de servicio a demandar, y a su vez que este sea capaz de capturar parámetros específicos de la red para que luego sean devueltos a la SIM y la misma se encargue de empaquetar e insertar esa información en un SMS, para que luego sea enviada a un número predefinido donde llegarán las solicitudes realizadas para su posterior procesamiento. Ese número predefinido será el de la aplicación tipo ESME descrita en el capítulo anterior, la cual es la que está a la espera de las solicitudes realizadas y se encarga del procesamiento de los datos enviados.

Descripción de los parámetros solicitados al móvil a través de la tarjeta SIM

SIM Application Toolkit

SIM Application Toolkit provee los mecanismos mediante los cuales aplicaciones residentes en la SIM interactúan y operan con cualquier teléfono móvil que soporta los comandos SIM Toolkit enviados por la aplicación. [3]

La aplicación a desarrollar está basada en comandos *SIM Toolkit* que le son enviados al teléfono para que devuelva información de interés que luego será utilizada para estimar los cálculos de ubicación. Hay que tener en cuenta que no todos los teléfonos soportan dichos comandos ya que dependen del tipo de fabricante y de la versión del equipo. La mayoría de los comandos son estándar, pero en el caso del desarrollo de la aplicación, existen comandos especiales que se le deben enviar al teléfono y que no todos lo soportan, debido a que son comandos muy específicos y poco comunes en el uso de aplicaciones. Toda la especificación técnica de los comandos SIM Toolkit se encuentran en la especificación GSM 11.14 de la ETSI (*European Telecommunications Institute*).

El comando STK utilizado para solicitar al móvil información concerniente de la red será el "*Provide Local Information*". A través de este comando la SIM le solicita al móvil información acerca su ubicación en la red, como por ejemplo: código del país donde está registrado (MCC), código de la red donde se encuentra (MNC), código de área donde está ubicado (LAC), el valor de la celda que le da servicio (CELL ID) y resultados de las mediciones realizadas por el móvil en la red (*Measurement Result*).

Parámetros que le son solicitados al móvil a través del comando STK "Provide Local Information"

- **Location Information**

Este parámetro está definido en 7 bytes. Los tres primeros bytes contienen el MCC (*Mobile Country Code*) y el MNC (*Mobile Network Code*). El MCC es el código que identifica a la red de Digitel a nivel mundial y fue establecido como el 734, y el MNC es el código que identifica a la red de Digitel a nivel nacional, en este caso es la 02. Los últimos 4 bytes definen el LAC y el CELL ID (Celda que da servicio al móvil), cada uno codificado en 2 bytes.

De todos los parámetros antes descritos solo se tomará el CELL ID, el cual es el único dato de todos los descritos que interesa para el cálculo de la ubicación.

En la siguiente figura se observa como está compuesto el *Location Information*.

LOCATION INFORMATION								
Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octeto 1
MCC digito 2				MCC digito 1				Octeto 1
1 1 1 1				MCC digito 3				Octeto 1
MNC digito 2				MNC digito 1				Octeto 1
LAC								Octeto 1
LAC (continuación)								Octeto 1
CELL ID								Octeto 1
CELL ID (continuación)								Octeto 1

Figura A1. Elementos que componen el Location Information

Para decodificar el valor del CELL ID arrojado se tiene que el bit 8 del octeto 8 es el más significante, y el bit 1 del octeto 7 es el menos significante. Al unir el octeto 8 con el 7 tenemos los valores de los posibles CELL ID acotados entre 0 y 65536. La codificación de los diferentes CELL ID es responsabilidad de cada administrador de la red y va depender de las configuraciones que este establezca para su operación.

- **Measurement Results**

Este parámetro se define en 17 bytes, y su propósito es proveer los resultados de las mediciones realizadas por el móvil en la celda servidora y celdas vecinas. [4]

La información más relevante de este parámetro se encuentra desde el octeto 4 hasta el octeto 17. En ellos se encuentran información concerniente a los niveles de potencia de la celda servidora y las celdas vecinas, el número de celdas vecinas que está monitoreando el móvil (máximo 6 celdas vecinas), el BCCH (*Broadcast Control Channel*) y el BSIC (*Base transceiver Station Identity Code*). Estos datos más el valor de la celda que presta servicio permiten descifrar la identidad de las celdas vecinas, es decir el CELL ID de las vecinas. Una vez con esto podemos saber la posición geográfica e identificar las celdas que están dando cobertura al móvil en ese momento.

En la siguiente figura se muestra como están estructurados los datos que arroja el parámetro *Measurement Result*.

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	
Measurement Results IEI								Octeto 1
BA- USED	DTX USED	RXLEV-FULL-SERVING-CELL						Octeto 2
0 SPARE	MEAS-VALID	RXLEV-SUB-SERVING-CELL						Octeto 3
0 SPARE	RXQUAL-FULL SERV ING-CELL			RXQUAL-SUB SERVING-CELL			NO-NCELL-M (High Part)	Octeto 4
NO-NCELL-M (Low Part)	RXLEV-NCELL 1							Octeto 5
BCCH-FREQ-NCELL 1					BSIC-NCELL 1 (High Part)			Octeto 6
BSIC-NCELL 1 (Low Part)	RXLEV-NCELL 2 (High Part)							Octeto 7
RXLEV NCELL 2 (Low Part)	BCCH-FREQ-NCELL 2					BSIC-NCELL 2 (High Part)		Octeto 8
BSIC-NCELL 2 (Low Part)	RXLEV-NCELL 3 (High Part)							Octeto 9
RXLEV NCELL 3 (Low Part)	BCCH-FREQ-NCELL 3					BSIC-NCELL 3 (High Part)		Octeto10
BSIC-NCELL 3 (Low Part)	RXLEV-NCELL 4 (High Part)							Octeto11
RXLEV NCELL 4 (Low Part)	BCCH-FREQ-NCELL 4							Octeto12
BSIC-NCELL 4						RXLEV-NCELL 5 (High Part)		Octeto13
RXLEV NCELL 5 (Low Part)	BCCH-FREQ-NCELL 5 (High Part)							Octeto14
BCCH-FREQ-NCELL 5 (Low Part)	BSIC-NCELL 5						RXLEV-NCELL 6 (High Part)	Octeto15
RXLEV-NCELL 6 (Low Part)	BCCH-FREQ-NCELL 6 (High Part)							Octeto16
BCCH-FREQ-NCELL 6 (Low Part)	BSIC-NCELL 6							Octeto17

Figura A2. Estructura de los datos contenidos por el parámetro Measurement Result

Descripción de la aplicación desarrollada en la tarjeta SIM

Software utilizado para el desarrollo de la aplicación en la SIM

En desarrollos de servicios basados en SIM, existe un amplio rango de productos disponibles para el diseño, desarrollo, simulación, test, edición y manejo de dichos servicios tales como: herramientas para desarrollo y simulación, una gama completa de tarjetas (tarjetas propietarias y open OS), una variedad de plataformas que permiten el manejo remoto y configuración de tarjetas, una variedad de gateway que permiten que las SIM sean provistas con un SIM browser para el acceso a contenido de Internet.

La aplicación desarrollada en la SIM fue realizada bajo un software propietario desarrollado por la empresa GEMPLUS. La herramienta de programación utilizada fue GemXplore, la cual ha sido diseñada especialmente para soportar avanzadas aplicaciones SIM Toolkit en SIM con capacidad de almacenamiento de 16/32 K y que se le quieran proveer de servicios de valor agregado.

Descripción del programa que extrae los parámetros de la red

La arquitectura del programa desarrollado es la siguiente:

(a) El usuario inicia la petición de solicitud de servicio.
(b) El programa residente en la SIM captura el tipo de servicio demandado mediante un menú que se despliega y ofrece un conjunto de opciones.
(c) Una vez capturada la solicitud el programa inicia la comunicación con el móvil.
(d) Establecida la comunicación se le envía al móvil el comando STK "*Provide Local Information*".
(e) El móvil empieza a estructurar la información solicitada (parámetros de la red) y la devuelve a la SIM.
(f) La SIM almacena momentáneamente dichos parámetros mientras se prepara para empaquetarlos en un SMS en un orden preestablecido.
(g) Una vez empaquetada la información solicitada y el tipo de servicio demandado, esta es insertada en un SMS para ser enviada a un número corto predefinido (número definido para la aplicación tipo ESME que recibe las solicitudes realizadas por los usuarios).
(h) Una vez enviado el SMS con la información concerniente, el programa vuelve al menú principal a la espera de nuevas solicitudes de servicio.

Este programa se inicia solo si el usuario realiza la solicitud, es decir; la SIM no interactúa por si sola con el equipo móvil. En este sentido el manejo de esta aplicación es unidireccional y se debe solicitar a la SIM que inicialice la aplicación.

En la figura A.3 se muestra el diagrama de flujo del programa residente en la SIM.

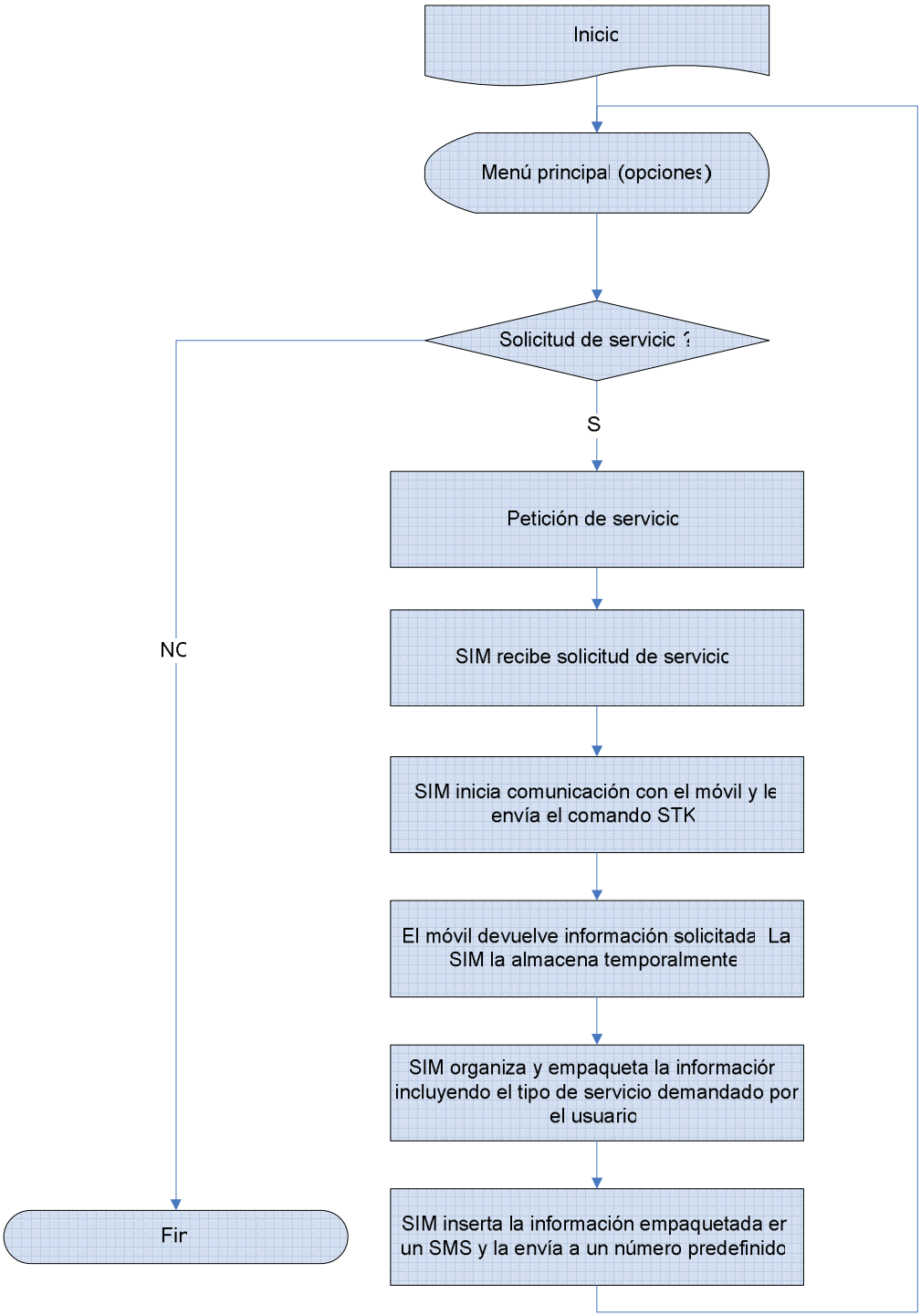

Figura A3. Diagrama de flujo del programa desarrollado en la SIM

Menú desarrollado a nivel de SIM

En principio se desarrollaron menús simples, es decir menús con pocas opciones a ofrecer; esto con la finalidad de probar el desarrollo del sistema y capturar los posibles errores cometidos en la aplicación. Una vez depurada la aplicación a nivel de SIM se fijó un menú de pruebas según las bases de datos de servicios disponibles para montar un demo de la aplicación.

El menú desarrollado para la comunicación del usuario con la aplicación es totalmente configurable, esto quiere decir que se puede ajustar a la necesidad del servicio a ofertar.

La estructura del menú desarrollado se muestra en la siguiente figura:

Figura A4. Estructura del menú desarrollado en la SIM

Como se observa en la figura anterior, el programa despliega un menú principal llamado “Ubicame” el cual está provisto de seis opciones posibles a elegir. Las posibles opciones son:

(a) Bancos
(b) Farmacias
(c) Hoteles
(d) Estaciones de servicio
(e) Restaurantes
(f) Sitios Turísticos

De todas las opciones solo la opción restaurantes despliega un submenú de servicios posibles. Estos servicios son:

(a) Italianos
(b) Españoles
(c) Chinos
(d) Areperas

De las categorías antes mencionadas se sobreentiende que estas corresponden a la de tipos de restaurantes.

Como ya se dijo antes, estos menús son totalmente configurables, todo va depender de los tipos de servicios que se quieran ofrecer y de la capacidad de almacenamiento en la SIM, ya que el programa ocupa un espacio en memoria y si la SIM no está en la capacidad de almacenarlo, dicha aplicación no puede ser cargada en ella. Otro aspecto importante es saber diferenciar el tipo de servicio solicitado por el usuario. Para esto a cada categoría se le diferencia dándole un valor único, es decir; estableciendo un diferenciador por servicio demandado. De esta manera la selección realizada por el usuario se marca de manera única y esta sirve como referencia a la aplicación tipo ESME que atiende las solicitudes enviadas. Así dicha aplicación podrá diferenciar y saber que servicio se solicitó a la hora de encontrar los servicios más cercanos y devolver el mensaje de respuesta.